PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-091816
(43)Date of publication of application : 29.03.2002

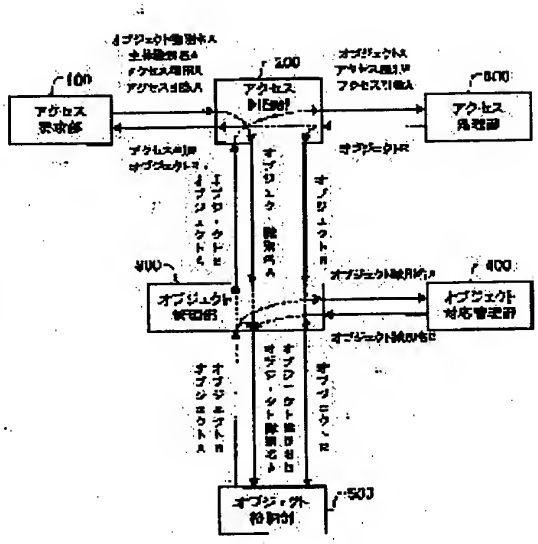
(51)Int.Cl. G06F 12/00
G06F 12/14
G06F 15/16

(21)Application number : 2000-274040
(22)Date of filing : 08.09.2000

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : KUDO MICHIHARU
AMANO TOMIO

(54) ACCESS CONTROL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an access control system capable of performing flexible control similar to access control to data even concerning access control to access control rules by handling the access control rules to data and the access control rules to the access control rules without distinction.
SOLUTION: This access control system is provided with an access control part 200 for deciding the propriety of access to an object corresponding to an access request based on access control rules specifying an access right to this object and an object storage part 500 storing the access control rules to this object as an object similar to a general data object and corresponding to the access request with the access control rule as a target,the access control part 200 decides the propriety of access to this access control rule.



LEGAL STATUS

[Date of request for examination]	10.07.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3790661
[Date of registration]	07.04.2006
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's	

decision of rejection]
[Date of extinction of right]

(2)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－91816
（P2002－91816A）
(43)公開日　平成14年３月29日(2002.3.29)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
G06F 12/00	537	G06F 12/00	537A 5B017
	547		547H 5B045
12/14	310	12/14	310K 5B082
15/16	620	15/16	620B

審査請求 有　請求項の数21 OL （全 25 頁）

(21)出願番号　特願2000－274040(P2000－274040)

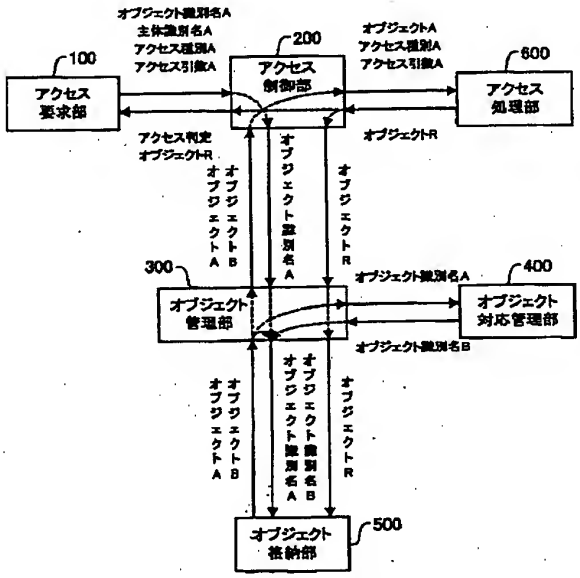
(22)出願日　平成12年９月８日(2000.9.8)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州
アーモンク　（番地なし）
(74)代理人　100086243
弁理士　坂口　博　（外４名）

最終頁に続く

(54)【発明の名称】　アクセス制御システム

(57)【要約】
【課題】　データに対するアクセス制御規則と、アクセス制御規則に対するアクセス制御規則とを区別することなく扱うことにより、アクセス制御規則に対するアクセス制御についても、データに対するアクセス制御と同様の柔軟な制御を行うことができるアクセス制御システムを提供する。
【解決手段】　アクセス制御システムにおいて、アクセス要求に応じて、このオブジェクトに対するアクセスの可否を、このオブジェクトに対するアクセス権限を規定したアクセス制御規則に基づいて判断するアクセス制御部２００と、このオブジェクトに対するアクセス制御規則を一般のデータオブジェクトと同様のオブジェクトとして格納したオブジェクト格納部５００とを備え、アクセス制御部２００は、アクセス制御規則を対象とするアクセス要求に応じて、このアクセス制御規則に対するアクセスの可否を判断する。



1

【特許請求の範囲】

【請求項１】　情報資源であるオブジェクトへのアクセス要求に対するアクセス制御を行うアクセス制御システムにおいて、

アクセス要求に応じて、前記オブジェクトに対するアクセスの可否を、当該オブジェクトに対するアクセス権限を規定したアクセス制御規則に基づいて判断するアクセス要求判断部と、

前記オブジェクトに対するアクセス制御規則をオブジェクトとして格納したオブジェクト格納部とを備え、

前記アクセス要求判断部は、アクセス制御規則を対象とするアクセス要求に応じて、当該アクセス制御規則に対するアクセスの可否を判断することを特徴とするアクセス制御システム。

【請求項２】　前記アクセス要求判断部は、

前記アクセス制御規則を含む所定の前記オブジェクトを対象とするアクセス要求に応じて、前記オブジェクト格納部から、当該アクセス要求の対象である前記オブジェクトと当該オブジェクトに対する前記アクセス制御規則とを取得し、

取得した前記アクセス制御規則に基づいて前記オブジェクトに対するアクセスの可否を判断する、請求項１に記載のアクセス制御システム。

【請求項３】　前記オブジェクト格納部にオブジェクトとして格納されるアクセス制御規則は、アクセス制御規則に対するアクセス権限を規定したアクセス制御規則である場合を含む、請求項１に記載のアクセス制御システム。

【請求項４】　アクセス要求の対象である前記オブジェクトと当該オブジェクトに対する前記アクセス制御規則との相互関係を管理するオブジェクト対応管理部をさらに備えた、請求項１に記載のアクセス制御システム。

【請求項５】　所定の情報資源へのアクセス要求に対するアクセス制御を行うアクセス制御システムにおいて、

前記情報資源へのアクセス権限を規定したアクセス制御規則と、当該アクセス制御規則と共通の書式で記述され、当該アクセス制御規則に対するアクセス権限を規定した上位制御規則とを格納した格納手段と、

前記アクセス制御規則を対象とするアクセス要求に応じて、当該アクセス制御規則に対するアクセスの可否を、前記上位制御規則に基づいて判断する判断手段とを備え、

前記格納手段に格納された前記アクセス制御規則は他のアクセス制御規則に対する前記上位制御規則である場合を含むことを特徴とするアクセス制御システム。

【請求項６】　前記格納手段に格納された前記アクセス制御規則は、前記上位制御規則を指し示す指示情報を付した指示情報付きオブジェクトとして記述される、請求項５に記載のアクセス制御システム。

【請求項７】　前記判断手段によりアクセスを許可されたアクセス要求に応じて、前記アクセス制御規則及び前記上位制御規則を生成し、変更し、または削除する処理手段をさらに備えた、請求項５に記載のアクセス制御システム。

【請求項８】　前記上位制御規則は、前記アクセス制御規則に対するアクセス権限の一部を特定の主体に対して認めることを規定した規則である、請求項５に記載のアクセス制御システム。

【請求項９】　データの構成要素に対する制御情報を示すタグを付されたタグ付きオブジェクトを対象とし、当該タグ付きオブジェクトへのアクセス要求に対するアクセス制御を行うアクセス制御システムにおいて、

前記タグ付きオブジェクトへのアクセス権限を規定するアクセス制御規則を格納したアクセス制御規則格納手段と、

アクセス要求に応じて、当該アクセス要求の対象である前記タグ付きオブジェクトに対するアクセスの可否を、前記アクセス制御規則に基づいて判断するアクセス要求判断手段とを備え、

前記アクセス制御規則格納手段に格納された前記アクセス制御規則は、規則の構成要素に対する制御情報を示すタグを付されたタグ付きオブジェクトとして記述され、

前記アクセス要求判断手段は、前記アクセス制御規則を対象とするアクセス要求に応じて、タグ付きオブジェクトである当該アクセス制御規則に対するアクセスの可否を判断することを特徴とするアクセス制御システム。

【請求項１０】　タグ付きオブジェクトとして記述されたタグ付きデータオブジェクトと前記タグを持たないタグ無しデータオブジェクトとを格納したデータオブジェクト格納手段をさらに備え、

前記アクセス要求判断手段は、前記アクセス制御規則、前記タグ付きデータオブジェクト、前記タグ無しデータオブジェクトのいずれかに対するアクセスの可否を判断する、請求項９に記載のアクセス制御システム。

【請求項１１】　前記タグ付きデータオブジェクトに対するアクセス要求が行われた場合に、当該タグ付きデータオブジェクトに対するアクセス制御規則に関する情報を保持する管理手段をさらに備え、

前記アクセス要求判断手段は、

前記タグ付きデータオブジェクトに付随する前記タグ無しデータオブジェクトに対するアクセス要求が行われた場合に、前記管理手段に保持されている情報に基づいて、当該タグ付きデータオブジェクトに対する前記アクセス制御規則を取得し、

取得した前記アクセス制御規則に基づいて前記タグ無しデータオブジェクトに対するアクセスの可否を判断する、請求項１０に記載のアクセス制御システム。

【請求項１２】　クライアントからのアクセス要求を受け付けて、アクセス対象であるオブジェクトに対して当該アクセス要求に応じた処理を行うサーバであって、

アクセス要求に応じて、当該アクセス要求の対象であるオブジェクトに対するアクセスの可否を、当該オブジェクトに対するアクセス権限を規定したアクセス制御規則に基づいて判断するアクセス要求判断部と、
前記アクセス要求判断部によりアクセスが許可されたアクセス要求に応じて、前記オブジェクトに対する処理を実行するオブジェクト処理部と、
前記オブジェクトに対するアクセス制御規則をオブジェクトとして格納したオブジェクト格納部とを備え、
前記アクセス要求判断部は、前記アクセス制御規則を対象とするアクセス要求に応じて、当該アクセス制御規則に対するアクセスの可否を判断することを特徴とするサーバ。

【請求項１３】　前記オブジェクト処理部は、前記アクセス制御規則を対象とするアクセス要求に応じて、前記アクセス制御規則を生成し、変更し、または削除する、請求項１２に記載のサーバ。

【請求項１４】　前記オブジェクト処理部は、前記アクセス制御規則を対象とするアクセス要求に応じて、アクセス制御規則に対するアクセス権限の一部を特定の主体に対して認めるアクセス制御規則を生成する、請求項１２に記載のサーバ。

【請求項１５】　情報資源であるオブジェクトへのアクセス要求に対するアクセス制御を行うアクセス制御方法において、
アクセス制御規則を対象オブジェクトとするアクセス要求を受け付けるステップと、
前記アクセス要求の対象オブジェクトに対するアクセス権限を規定するアクセス制御規則を取得するステップと、
取得した前記アクセス制御規則に基づいて前記対象オブジェクトに対するアクセスの可否を判定するステップとを含む、アクセス制御方法。

【請求項１６】　データの構成要素に対する制御情報を示すタグを付されたタグ付きオブジェクトを対象とし、当該タグ付きオブジェクトへのアクセス要求に対するアクセス制御を行うアクセス制御方法において、
前記タグ付きオブジェクトに対するアクセス要求が行われた場合に、当該タグ付きオブジェクトに対するアクセス制御規則に関する情報を保持するステップと、
前記タグ付きオブジェクトに付随するタグ無しオブジェクトに対するアクセス要求が行われた場合に、前記アクセス制御規則に関する情報を保持するステップにおいて保持された情報に基づいて当該タグ付きオブジェクトに対するアクセス制御規則を取得するステップと、
取得された前記アクセス制御規則を用いて前記タグ無しオブジェクトに対するアクセスの可否を行うステップとを含む、アクセス制御方法。

【請求項１７】　情報資源であるオブジェクトへのアクセス要求に対するアクセス制御を行うためのアクセス制御規則を生成するアクセス制御規則生成方法において、
前記アクセス制御規則の生成要求を受け付け、当該生成要求に対する前記アクセス制御規則に基づいて、当該生成要求を許可するかどうかを判断するステップと、
前記生成要求が許可された場合に、当該生成要求に応じたアクセス制御規則を生成し、前記生成要求に対するアクセス制御規則を指示する指示情報を生成された当該アクセス制御規則に付加するステップとを含む、アクセス制御規則生成方法。

【請求項１８】　コンピュータに実行させるプログラムを当該コンピュータの入力手段が読取可能に記憶した記憶媒体において、
前記プログラムは、
アクセス制御規則を対象オブジェクトとするアクセス要求を受け付ける処理と、
前記アクセス要求の対象オブジェクトに対するアクセス権限を規定するアクセス制御規則を取得する処理と、
取得した前記アクセス制御規則に基づいて前記対象オブジェクトに対するアクセスの可否を判定する処理とを前記コンピュータに実行させる、記憶媒体。

【請求項１９】　コンピュータに実行させるプログラムを当該コンピュータの入力手段が読取可能に記憶した記憶媒体において、
前記プログラムは、
所定の情報資源に対するアクセス権限を規定するアクセス制御規則の生成要求を受け付け、当該生成要求に対するアクセス制御を行うためのアクセス制御規則に基づいて、当該生成要求を許可するかどうかを判断する処理と、
前記生成要求が許可された場合に、当該生成要求に応じたアクセス制御規則を生成し、前記生成要求に対する前記アクセス制御規則を指示する指示情報を生成された当該アクセス制御規則に付加する処理とを前記コンピュータに実行させる、記憶媒体。

【請求項２０】　コンピュータに、アクセス制御規則を対象オブジェクトとするアクセス要求を受け付ける処理と、前記アクセス要求の対象オブジェクトに対するアクセス権限を規定するアクセス制御規則を取得する処理と、取得した前記アクセス制御規則に基づいて前記対象オブジェクトに対するアクセスの可否を判定する処理とを実行させるプログラムを記憶する記憶手段と、
前記記憶手段から前記プログラムを読み出して当該プログラムを送信する送信手段とを備えた、プログラム伝送装置。

【請求項２１】　コンピュータに、所定の情報資源に対するアクセス権限を規定するアクセス制御規則の生成要求を受け付け、当該生成要求に対するアクセス制御を行うためのアクセス制御規則に基づいて、当該生成要求を許可するかどうかを判断する処理と、前記生成要求が許可された場合に、当該生成要求に応じたアクセス制御規

則を生成し、前記生成要求に対する前記アクセス制御規則を指示する指示情報を生成された当該アクセス制御規則に付加する処理とを実行させるプログラムを記憶する記憶手段と、

前記記憶手段から前記プログラムを読み出して当該プログラムを送信する送信手段とを備えた、プログラム伝送装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、アクセス制御に関し、特にアクセス制御規則を柔軟に設定するためのアクセス制御規則に対するアクセス制御に関する。

【０００２】

【従来の技術】今日、コンピュータのセキュリティの観点から、情報資源であるオブジェクト（データファイルやディレクトリなど）に対するアクセス制御が一般に行われている。アクセス制御は、所定のオブジェクトに対してアクセス権限を持つ者やアクセスできる内容（実行できる処理の種類）を制限するアクセス制御規則を設定し、この規則に基づいて、ユーザなどからのアクセス要求を評価し、アクセスの可否を判断する。

【０００３】このようなアクセス制御を行うことのできる代表的な例としてＯＳ(OperatingSystem)のＵＮＩＸ（登録商標）がある。ＵＮＩＸにおいては、ファイルシステムやユーザＩＤ等を使用してアクセス制御が行われている。ファイルシステムには、所有者(owner)、所有者の所属するグループ(group)、その他(other)の三種類のサブジェクトがある。そして各サブジェクトに対してそれぞれ、ファイルの読込み(read)、書込み(write)、実行(execute)権限の可否が指定されている。これら全ての権限を制限なく行使できるのは、全ての権限を持っているスーパーユーザである、ルート(root)ユーザでなければならない。また、それぞれのユーザＩＤ毎のデータに制限なくアクセスすることができるのも、全ての権限を持っているスーパーユーザである、rootユーザでなければならない。これらは、最上位の固定されたアクセス制御規則により決定されている。そして、このrootユーザが持っている権限の一部を他のユーザに委譲したりすることはできない。この為、他のユーザに対してrootユーザの持つような強い権限を与えようとする場合には、root権限そのものを与える必要がある。

【０００４】また、他のアクセス制御の例として、アプリケーションソフトウェア自身が管理するオブジェクトに対するアクセス制御を行う例がある。例えば、データベース、ビュー、フォーム、文書などの複数オブジェクトの階層に対して柔軟にアクセス制御を付加することができるソフトウェアとして、米国ロータス社のNotesが知られている。このNotesによるアクセス制御規則の変更権限はデータベース管理者のロールにのみ固定的に与えられている。つまり、データベース管理者のロールに

ユーザを追加すれば、皆がアクセス制御規則を変更することができる。しかしながら、一部のオブジェクト階層にのみ変更権限を持たせ、他の部分のオブジェクト階層には変更権限を持たせないようなアクセス制御を行うことはできない。

【０００５】以上の例のように、従来のアクセス制御システムにおいて、一般に、アクセス制御規則に対するアクセス権限に関して、ユーザは、全ての権限が与えられるか、全く何の権限も持つことができないかのどちらかであった。

【０００６】また、アクセス制御規則を記述するための言語に関する従来技術としてＢＪＳがある。このＢＪＳでは、administration権限に基づいてアクセス制御規則に対するアクセス制御規則を管理することができる。administration権限にはadministerとadm-accessの２種類がある。administerはadministration権限を含む全てのアクセス制御規則を作成することができ、adm-accessはadminister権限とadm-access権限とを除く他の権限（selectやcreateなど）を持つアクセス制御規則を作成することができる。例えば、adm-access権限を持つAliceに関して、次のアクセス制御規則が存在するとする。

<Alice, select, adm-access, strong, table1, Trent>

このアクセス制御規則は、Aliceがtable1のselect操作に関する限り、アクセス制御規則を自由に生成し、削除することができることを意味する。例えば、Employeeがtable1にselectに関する権限を持ち、この権限の作成者がAliceであることを示す規則、

<Employee, select, +, table1, Alice, strong>

を作成することができる。他の例としては、例えば、administer権限を持つBobに関して、次のアクセス制御規則が存在するとする。

<Bob, select, administrater, strong, table1, Trent>

このアクセス制御規則は、Bobがtable1のselect操作に関する限り、アクセス制御規則の作成権限を他人に委譲することができることを意味する。例えば、Carolがtable1にselect操作権限に関する限り、Carolがtable1にselect操作権限に関するアクセス制御規則を作成する権限を持ち、この権限の作成者がBobであることを示す規則、

<Carol, select, adm-access, strong, table1, Bob>

を作成することができる。

【０００７】ＢＪＳを用いれば、上記のようにアクセス制御規則に対するアクセスを制御する規則を記述することができる。ただし、アクセス制御規則の記述と、アクセス制御規則に対するアクセス制御規則であるadministration権限の記述とは、異なる書式で行われる。

【０００８】

【発明が解決しようとする課題】上述したように、従来、オペレーティングシステムやアプリケーションソフ

トウェアにて行われている一般的なアクセス制御は、アクセス制御規則自体に対するアクセス権限に関して、ユーザは、全ての権限を与えられるか、全く何の権限も持つことができないかのどちらかであった。そのため、特定のアクセス制御規則の追加のみを特定のユーザに与えるというように、アクセス制御規則に対するアクセス権限を制限付きで認めることができなかった。すなわち、アクセス制御規則に対するアクセス権限の一部を委譲することはできなかった。そして、多くのユーザにアクセス制御規則に対する全てのアクセス権限を与えてしまうことは、セキュリティ上好ましくない。また、システムに変更があった場合に、権限の管理が煩雑となる。

【０００９】また、ＢＪＳを用いることにより、上述したように、アクセス制御規則に対するアクセスを制御する規則を記述することが可能となる。しかし、ＢＪＳにおいて、administration権限は、アクセス制御規則とは異なる書式で記述されており、その内容を、当該administration権限により制御されるアクセス制御規則の対象であるオブジェクト（tableなど）との組で決めなければならない。したがって、例えば特定のオブジェクトに対して指定されたアクセス制御規則を見る権限（readなど）などのように、アクセス制御規則に対する権限の内容がオブジェクトと分離されているような権限を設定することはできない。このように、ＢＪＳを用いてアクセス制御規則に対するアクセスを制御しようとする場合にも、柔軟なアクセス制御を行うことができない。

【００１０】これら従来のアクセス制御における問題点を解決し、ユーザに対して、アクセス制御規則に対する権限の任意の一部を与えることができれば、より使いやすく便利なアクセス制御システムとして活用できる。また、アクセス制御規則に対するアクセスを制御する規則として、アクセス制御規則の追加、変更、削除等の記述を柔軟に行うことができれば、更に使いやすく便利なアクセス制御システムとして活用できる。

【００１１】そこで本発明は、データに対するアクセス制御規則と、アクセス制御規則に対するアクセス制御規則とを区別することなく扱うことにより、アクセス制御規則に対するアクセス制御についても、データに対するアクセス制御と同様の柔軟な制御を行うことができるアクセス制御システムを提供することを目的とする。これにより、ユーザに対して、アクセス制御規則に対する権限の任意の一部を与えるようなアクセス制御を容易に行うことが可能となる。また、アクセス制御規則の追加、変更、削除等を容易に行うことが可能となる。

【００１２】

【課題を解決するための手段】上記の目的を達成するため、本発明は、情報資源であるオブジェクトへのアクセス要求に対するアクセス制御を行うアクセス制御システムにおいて、アクセス要求に応じて、このオブジェクトに対するアクセスの可否を、このオブジェクトに対するアクセス権限を規定したアクセス制御規則に基づいて判断するアクセス要求判断部と、このオブジェクトに対するアクセス制御規則を一般のデータオブジェクトと同様のオブジェクトとして格納したオブジェクト格納部とを備え、アクセス要求判断部は、アクセス制御規則を対象とするアクセス要求に応じて、このアクセス制御規則に対するアクセスの可否を判断することを特徴とする。すなわち、アクセス制御規則を一般のデータオブジェクトと区別することなく扱うことができる。

【００１３】ここで、このアクセス要求判断部は、このアクセス制御規則を含む所定のオブジェクトを対象とするアクセス要求に応じて、オブジェクト格納部から、このアクセス要求の対象であるオブジェクトとこのオブジェクトに対するアクセス制御規則を記述したオブジェクトとを取得し、取得したアクセス制御規則に基づいてこのオブジェクトに対するアクセスの可否を判断することを特徴とする。すなわち、アクセス要求判断部は、オブジェクト格納部からアクセス対象とアクセス制御規則の二つのオブジェクトを取得し、これらを用いてアクセス要求に対するアクセスの可否を判断する。

【００１４】さらにここで、このオブジェクト格納部にオブジェクトとして格納されるアクセス制御規則は、同じくオブジェクト格納部に格納されている他のアクセス制御規則に対するアクセス権限を規定したアクセス制御規則である場合を含む。言い換えれば、アクセス制御規則に対するアクセス制御規則もオブジェクトとしてアクセス要求の対象となり、さらに上位のアクセス制御規則によってアクセス制御されるという多重化された構造を取り得る。

【００１５】また、このアクセス制御システムにおいて、アクセス要求の対象であるオブジェクトとこのオブジェクトに対するアクセス制御規則との相互関係を管理するオブジェクト対応管理部をさらに備えた構成とすることができる。具体的には、このオブジェクト対応管理部は、アクセス制御規則との対応が記述されたオブジェクトからこの対応情報を取得して管理する。そして、このオブジェクトに付随し、かつアクセス制御規則との対応が記述されていないオブジェクトに対してアクセス要求がなされた場合に、このオブジェクト対応管理部により保管されていたアクセス制御規則の対応情報に基づいてアクセス制御規則を取得し、このアクセス制御規則との対応が記述されていないオブジェクトに対するアクセス制御規則として用いることができる。オブジェクトとアクセス制御規則との対応情報は、オブジェクトに付するタグにより記述することができる。

【００１６】また、本発明は、他のアクセス制御システムを提供することができる。すなわち、所定の情報資源へのアクセス要求に対するアクセス制御を行うアクセス制御システムにおいて、この情報資源へのアクセス権限を規定したアクセス制御規則と、このアクセス制御規則

と共通の書式で記述され、かつこのアクセス制御規則に対するアクセス権限を規定した上位制御規則とを格納した格納手段と、このアクセス制御規則を対象とするアクセス要求に応じて、このアクセス制御規則に対するアクセスの可否を、この上位制御規則に基づいて判断する判断手段とを備える。そして、この格納手段に格納されたアクセス制御規則は他のアクセス制御規則に対する上位制御規則である場合を含むことを特徴とする。すなわち、アクセス制御規則もアクセス要求の対象となる一つの情報資源としてみた場合に上位制御規則もアクセス制御規則に他ならない。したがって、共通の書式でアクセス制御規則を記述し、その制御対象を他のアクセス制御規則とすることによって、上位制御規則を作成することができ、アクセス制御規則を多重化することができる。

【００１７】ここで、この格納手段に格納されたアクセス制御規則は、一般のデータオブジェクトにおいてアクセス制御規則を指し示す指示情報を付加するのと同様に、自アクセス制御規則に対する上位制御規則を指し示す指示情報を付した指示情報付きオブジェクトとして記述することができる。この指示情報は上述したタグで表現することができる。

【００１８】また、このアクセス制御システムは、判断手段によりアクセスを許可されたアクセス要求に応じて、このアクセス制御規則及びこの上位制御規則を生成し、変更し、または削除する処理手段をさらに備えた構成とすることができる。

【００１９】さらにここで、この上位制御規則は、このアクセス制御規則に対するアクセス権限の一部を特定の主体に対して認めることを規定した規則とすることができる。

【００２０】また、本発明は、さらに他のアクセス制御システムを提供することができる。すなわち、データの構成要素に対する制御情報を示すタグを付されたタグ付きオブジェクトを対象とし、当該タグ付きオブジェクトへのアクセス要求に対するアクセス制御を行うアクセス制御システムにおいて、このタグ付きオブジェクトへのアクセス権限を規定するアクセス制御規則を格納したアクセス制御規則格納手段と、このアクセス要求に応じて、このアクセス要求の対象であるタグ付きオブジェクトに対するアクセスの可否を、このアクセス制御規則に基づいて判断するアクセス要求判断手段とを備え、このアクセス制御規則格納手段に格納されたアクセス制御規則は、規則の構成要素に対する制御情報を示すタグを付されたタグ付きオブジェクトとして記述され、このアクセス要求判断手段は、このアクセス制御規則を対象とするアクセス要求に応じて、タグ付きオブジェクトであるこのアクセス制御規則に対するアクセスの可否を判断することを特徴とする。すなわち、アクセス制御規則をタグ付きオブジェクトの形式で記述したことにより、アクセス制御システム上は、ＨＴＭＬなどの一般のタグ付きデータオブジェクトとアクセス制御規則とを区別することなく扱うことができる。

【００２１】ここで、このアクセス制御システムは、タグ付きオブジェクトとして記述されたタグ付きデータオブジェクトと前記タグを持たないタグ無しデータオブジェクトとを格納したデータオブジェクト格納手段をさらに備え、アクセス要求判断手段は、アクセス制御規則、タグ付きデータオブジェクト、タグ無しデータオブジェクトのいずれかに対するアクセスの可否を判断することを特徴とする。

【００２２】さらにここで、このアクセス制御システムは、このタグ付きデータオブジェクトに対するアクセス要求が行われた場合に、このタグ付きデータオブジェクトに対するアクセス制御規則に関する情報を保持する管理手段をさらに備え、アクセス要求判断手段は、このタグ付きデータオブジェクトに付随するタグ無しデータオブジェクトに対するアクセス要求が行われた場合に、この管理手段に保持されている情報に基づいて、このタグ付きデータオブジェクトに対するアクセス制御規則を取得し、取得したこのアクセス制御規則に基づいてこのタグ無しデータオブジェクトに対するアクセスの可否を判断する構成とすることができる。すなわち、データオブジェクトをタグ付きデータオブジェクトとタグ無しデータオブジェクトとに分け、タグ無しデータオブジェクトはこのオブジェクトが付随するタグ付きデータオブジェクトのアクセス制御規則を流用することにより、タグ無しデータオブジェクトへのアクセス制御を実現できる。

【００２３】また、本発明は、クライアントからのアクセス要求を受け付けて、アクセス対象であるオブジェクトに対してこのアクセス要求に応じた処理を行うサーバであって、アクセス要求に応じて、このアクセス要求の対象であるオブジェクトに対するアクセスの可否を、当該オブジェクトに対するアクセス権限を規定したアクセス制御規則に基づいて判断するアクセス要求判断部と、このアクセス要求判断部によりアクセスが許可されたアクセス要求に応じて、このオブジェクトに対する処理を実行するオブジェクト処理部と、このオブジェクトに対するアクセス制御規則をオブジェクトとして格納したオブジェクト格納部とを備え、このアクセス要求判断部は、このアクセス制御規則を対象とするアクセス要求に応じて、このアクセス制御規則に対するアクセスの可否を判断することを特徴とする。すなわち、アクセス制御を行ってオブジェクトに対する処理を行うサーバとして提供することができる。

【００２４】また、本発明は、情報資源であるオブジェクトへのアクセス要求に対するアクセス制御を行うアクセス制御方法において、アクセス制御規則を対象オブジェクトとするアクセス要求を受け付けるステップと、このアクセス要求の対象オブジェクトに対するアクセス権限を規定するアクセス制御規則を取得するステップと、

取得したこのアクセス制御規則に基づいてこの対象オブジェクトに対するアクセスの可否を判定するステップとを含むことを特徴とする。すなわち、アクセス制御規則を一般のデータオブジェクトと同様に対象オブジェクトとしてアクセス要求を受け付け、アクセス制御を行うことができる。

【００２５】さらにまた、本発明は、データの構成要素に対する制御情報を示すタグを付されたタグ付きオブジェクトを対象とし、このタグ付きオブジェクトへのアクセス要求に対するアクセス制御を行うアクセス制御方法において、このタグ付きオブジェクトに対するアクセス要求が行われた場合に、このタグ付きオブジェクトに対するアクセス制御規則に関する情報を保持するステップと、このタグ付きオブジェクトに付随するタグ無しオブジェクトに対するアクセス要求が行われた場合に、このアクセス制御規則に関する情報を保持するステップにおいて保持された情報に基づいてこのタグ付きオブジェクトに対するアクセス制御規則を取得するステップと、取得されたアクセス制御規則を用いてこのタグ無しオブジェクトに対するアクセスの可否を行うステップとを含むことを特徴とする。

【００２６】また、本発明は、情報資源であるオブジェクトへのアクセス要求に対するアクセス制御を行うためのアクセス制御規則を生成するアクセス制御規則生成方法において、このアクセス制御規則の生成要求を受け付け、この生成要求に対する前記アクセス制御規則に基づいて、この生成要求を許可するかどうかを判断するステップと、この生成要求が許可された場合に、この生成要求に応じたアクセス制御規則を生成し、この生成要求に対するアクセス制御規則を指示する指示情報を生成されたこのアクセス制御規則に付加するステップとを含むことを特徴とする。

【００２７】さらに本発明は、これらのアクセス制御方法またはアクセス制御規則生成方法における各ステップに相当する処理をコンピュータに実行させるプログラムを作成し、コンピュータにて読み取り可能な記憶媒体に格納して提供したり、プログラム伝送装置から配信したりすることにより提供することができる。

【００２８】

【発明の実施の形態】以下、添付図面に示す実施の形態に基づいて本発明を詳細に説明する。まず、本発明の概要について説明する。本発明は、通常のアクセス制御の対象であるオブジェクトとアクセス制御規則自体とを区別することなく扱うため、タグ付きオブジェクトという概念を導入した。ここで、タグとは、データの構成要素に対する制御情報を示すデータであり、例えば、データの構成要素に対して付けられた固有の名前とすることができる。また、タグ付きオブジェクトとは、タグ名によりデータを参照することができるようなオブジェクトである。例えば、ＨＴＭＬ（Hypertext Markup Languag e）やＸＭＬ（Extensible Markup Language）などのマークアップ言語はオブジェクトである。

【００２９】本発明では、アクセス制御規則をタグ付きオブジェクトとして記述する。また、一般のデータオブジェクトについてもタグ付きオブジェクトとタグを持たないタグ無しオブジェクトとに分類する。そして、オブジェクトの記述形式に応じたアクセス制御を行う。これにより、タグ付きオブジェクトであれば、アクセス制御規則であるかデータオブジェクトであるかに関わらず、同様の手法でアクセス制御を行うことが可能となる。

【００３０】図１は、本実施の形態における、アクセス制御システムの全体構成を説明する図である。図１において、符号１００はアクセス要求部であり、アクセス要求を発行する。符号２００はアクセス制御部であり、管理している情報資源であるオブジェクトに対するアクセスの可否を制御するアクセス要求判断手段である。符号３００はオブジェクト管理部であり、オブジェクトやアクセス制御規則をオブジェクト格納部（後述の符号５００）から取り出して、アクセス制御部２００に渡す。また、オブジェクト格納部５００から取り出されたオブジェクトやアクセス制御規則を補足するために、必要に応じてオブジェクト対応管理部（後述の符号４００）を使うことができる。符号４００はオブジェクト対応管理部であり、オブジェクト格納部５００からオブジェクトを取り出す際、またはオブジェクト格納部５００に対してオブジェクトを格納する際に、当該オブジェクトの状態を管理する。特に、取り出されたオブジェクトに対するアクセス制御規則などの情報を一時的に蓄える機能を持つ。符号５００はオブジェクト格納部であり、アクセス要求の対象となるオブジェクトを格納している。符号６００はアクセス処理部６００であり、アクセス制御部２００によって許可されたアクセス要求に応じて、当該アクセス制御の対象であるオブジェクトに対する処理を実行する。

【００３１】本実施の形態におけるアクセス制御システムは、複数のコンピュータ装置をネットワークで接続したネットワークシステムとして構築されても良いし、単一のコンピュータ装置の一部として構成されても良い。前者の場合、例えば図１に示すアクセス要求部１００は、パーソナルコンピュータや携帯端末、その他の各種の端末装置にて実現される。そして、アクセス制御部２００、オブジェクト管理部３００、オブジェクト対応管理部４００、オブジェクト格納部５００及びアクセス処理部６００は、アクセス要求部１００である端末装置にネットワークを介して接続されたサーバマシンにて実現される。また、後者の場合、例えばアクセス要求部１００は、コンピュータ装置内で動作し、オブジェクト格納部５００に格納されているオブジェクトに対してアクセスし、処理を行うアプリケーションプログラムの機能により実現される。そして、アクセス制御部２００、オブ

ジェクト管理部３００、オブジェクト対応管理部４００、オブジェクト格納部５００及びアクセス処理部６００は、オペレーティングシステムやアプリケーションプログラムの機能により実現される。なお、図１に示す各構成要素は、上記アプリケーションプログラムやオペレーティングシステムなどのコンピュータプログラムにて制御されたＣＰＵにて実現される仮想的なソフトウェアブロックである。ＣＰＵを制御する当該コンピュータプログラムはＣＤ－ＲＯＭやフロッピー（登録商標）ディスクなどの記憶媒体に格納したり、ネットワークを介して伝送したりすることにより提供される。

【００３２】また、オブジェクト格納部５００に格納されるオブジェクトは、タグを付されたタグ付きオブジェクトとタグを持たないタグ無しオブジェクトからなる。タグ付きオブジェクトには、文書など一般のデータであるタグオブジェクトとタグ付きオブジェクトに対するアクセス制御規則を記述したアクセス制御タグオブジェクトとがある。アクセス制御タグオブジェクトには、タグオブジェクトのみならず、他のアクセス制御タグオブジェクトに対するアクセス制御規則を記述したものも存在する。タグ無しオブジェクトは、内部にタグ表現を持たない任意の形式のオブジェクトである。

【００３３】図２は図１に示したアクセス制御システムにおける動作のアルゴリズムの全体概要を表している。まず、アクセス要求部１００によって、オブジェクトに対するアクセス要求が生成される（ステップ７０１）。ステップ７０１においてアクセス要求部１００で生成されたアクセス要求は、アクセス制御部２００へ送られる。アクセス制御部２００を受け取ったアクセス要求は、オブジェクト管理部３００を介してオブジェクト格納部５００からアクセス要求の対象となるオブジェクトを取り出す（ここでは、アクセス要求の対象としてアクセス制御タグオブジェクト、タグオブジェクト、タグ無しオブジェクトの３種類が考えられるため、単にオブジェクトと表記する）。オブジェクト管理部３００は、アクセス対象であるオブジェクトと共に、当該オブジェクトに対するアクセス制御規則を記述したアクセス制御タグオブジェクトをオブジェクト格納部５００から取り出し、アクセス制御部２００へ送る。この際、必要であれば、取り出されたオブジェクトに対してオブジェクト対応管理部４００に処理を渡し、補足処理を行う。

【００３４】アクセス対象であるオブジェクト及びアクセス制御タグオブジェクトを受け取ったアクセス制御部２００は、当該オブジェクトに対するアクセスの可否を判定する（ステップ７０２）。ステップ７０２においてアクセスが許可されると、アクセス処理部６００が、アクセス要求の対象であるオブジェクトに対し、アクセス要求に応じた処理を施す（ステップ７０３）。ステップ７０３において処理が施されたオブジェクトは、当該処理の内容に応じてアクセス制御部２００によって返送先を判断され、アクセス要求部１００またはオブジェクト格納部５００に送られる（ステップ７０４）。例えば、アクセス要求としてデータのリードを要求した場合は、対象であるオブジェクトはアクセス要求部１００に返送される必要がある。また、アクセス要求に応じた処理としてデータの書き換えが行われた場合は、書き換えられたオブジェクトをオブジェクト格納部５００に格納する必要がある。以上のように、図１に示すアクセス制御システムにおける主要な処理の流れは、アクセス対象がアクセス制御規則であるアクセス制御タグオブジェクトであると、一般のデータオブジェクトであるタグオブジェクトまたはタグ無しオブジェクトであるとを問わず同一である。

【００３５】図３は、本実施の形態においてアクセス対象となるオブジェクトのデータ構造を説明する図である。これらはオブジェクト格納部５００に格納されるオブジェクトであり、上述したように、タグ付きオブジェクトとタグ無しオブジェクトとからなる。タグ付きオブジェクトはさらに、一般のデータオブジェクトであるタグオブジェクトと、タグがアクセス制御の内容に関する規則を規定しているアクセス制御タグオブジェクトとに分けられる。タグ付きオブジェクトのデータ構造は、タグにより、図３に示すように特定される。

【００３６】図３を参照すると、タグオブジェクトに付されるタグには、アクセス制御識別名タグと、アクセス可能主体タグと、その他の任意のタグとがある。アクセス制御識別名タグは、自タグオブジェクトに対するアクセス制御規則を記述したアクセス制御タグオブジェクトを指示する、オブジェクトＩＤ等の識別名を示すタグである。アクセス可能主体タグは、タグオブジェクトを生成したアクセス主体であるユーザ名、グループ名、システムプロセス番号等を指示するタグである。当該タグにて示されるアクセス可能主体は、当該タグオブジェクトに対して行うことができる処理の全てに対してアクセス権限を持つ。また、タグオブジェクトには、当該タグオブジェクトのデータ形式などに応じてデータ構造を示す任意のタグを設定することができる。なお、アクセス制御識別名タグ及びアクセス可能主体タグは、一つのタグオブジェクトに対してそれぞれ複数設定することができる。

【００３７】次に、アクセス制御タグオブジェクトに付されるタグには、アクセス制御識別名タグと、アクセス可能主体タグと、アクセス対象タグと、アクセス主体タグと、アクセス種別タグと、アクセスフラグタグと、アクセス条件タグとがある。このうち、アクセス制御識別名タグとアクセス可能主体タグとは、タグオブジェクトにおいて上述した各タグと同一である。アクセス対象タグは、当該アクセス制御タグオブジェクトによるアクセス制御の対象となるオブジェクト（以下、対象オブジェクト）を示すタグである。当該アクセス対象タグの内容

は対象オブジェクトに付されたタグのタグ名である。複数のオブジェクトによってタグの親子関係を示している場合、タグ名を使うことによりアクセス対象のオブジェクトを決めることができる。アクセス主体タグは、当該アクセス制御タグオブジェクトにより対象オブジェクトへのアクセスを許可されている主体を示すタグである。当該アクセス主体タグの内容は、対象オブジェクトへのアクセスを行うユーザ、グループ、プロセスなどを特定する識別子である。アクセス種別タグは、対象オブジェクトに対して行う処理の種類を示すタグである。処理の例としては、読出し、変更、追加、生成、削除などがある。アクセスフラグタグは、アクセスの可否を決めるフラグであり、その内容は、許可と不許可である。すなわち、アクセス要求において、アクセス主体タグにて示されているアクセス主体が、アクセス対象タグにて示されている対象オブジェクトを対象として、アクセス種別タグに示されている処理を要求した場合、アクセスフラグタグが許可となっていれば、当該アクセス制御タグオブジェクトは、そのようなアクセスを許可する。一方、アクセスフラグタグが不許可となっていれば、当該アクセス制御タグオブジェクトは、そのようなアクセスを拒否する。アクセス条件タグは、アクセス制御タグオブジェクトを適用する条件を示すタグであり、何らかの評価可能な条件式として記述される。なお、アクセス制御タグオブジェクトを構成するタグのうち、アクセス対象タグ、アクセス主体タグ、アクセス種別タグ、アクセスフラグタグ及びアクセス条件タグが一組となって、一つのアクセス制御規則を表現する。したがって、この組を複数設定することにより、当該アクセス制御タグオブジェクトに同種のアクセス制御規則を複数設定することができる。なお、各組において、アクセス条件タグなど、特に設定しなくてもアクセス制御に差し支えないタグについては、内容をＮＵＬＬとすることもできる。また、これらのタグの種類は一例に過ぎず、アクセス制御に差し支えなければ、いずれかのタグを省略しても良いし、アクセス制御のために用いることができる情報であれば、他のタグを追加しても良い。以上のように、本実施の形態では、アクセス制御規則を、タグによりデータ構造を特定されたタグ付きオブジェクトとして記述することにより、上述したタグオブジェクトと同様に扱うことが可能となる。

【００３８】タグ無しオブジェクトは、任意の形式のオブジェクトであり、内部にタグによって表現されるデータ構造を持たない。例えばＧＩＦファイルなどはタグ無しオブジェクトである。

【００３９】図４は、図１に示したアクセス制御システムの各ブロック間でやりとりされる情報（インターフェイス）の一覧を示す図である。図４を参照すると、アクセス要求部１００からアクセス制御部２００の方向には、アクセス要求が送られる。ここで、アクセス要求とは、アクセス対象、アクセス主体、アクセス種別からなる三つのデータの組であり、例えば上述したタグのタグ名を記述する。アクセス制御部２００からアクセス要求部１００の方向には、アクセス制御の判定結果を表すアクセスフラグの情報と、アクセス処理部６００にて処理されたオブジェクトが送られる。アクセス制御部２００からオブジェクト管理部３００の方向には、アクセス対象を表すオブジェクト識別子が送られる。ここで、オブジェクト識別子とは、オブジェクトを一意に参照する情報であり、例えば、オブジェクトＩＤやXPathなどの表現形式を持つ。また、アクセス制御部２００からオブジェクト格納部５００の方向には、アクセス処理部６００にて処理されたオブジェクトが送られる。オブジェクト管理部３００からアクセス制御部２００の方向には、対象オブジェクトとアクセス制御タグオブジェクトが送られる。オブジェクト管理部３００からオブジェクト格納部５００の方向には、アクセス対象を表すオブジェクト識別子が送られる。オブジェクト格納部５００からオブジェクト管理部３００の方向には、対象オブジェクトまたはアクセス制御タグオブジェクトが送られる。オブジェクト管理部３００からオブジェクト対応管理部４００の方向には、対象オブジェクトやアクセス制御タグオブジェクトを表すオブジェクト識別子が送られる。オブジェクト対応管理部４００からオブジェクト管理部３００の方向には、アクセス制御タグオブジェクトが送られる。アクセス制御部２００からアクセス処理部６００の方向には、処理対象であるオブジェクトと、アクセス制御タグオブジェクトから取得されるアクセス対象タグ、アクセス種別タグ及びアクセスフラグとが送られる。また、アクセス処理部６００からアクセス制御部２００の方向には処理済みのオブジェクトが送られる。

【００４０】次に、図１を用いて、本実施の形態を各構成要素とそれに伴うオブジェクトの動きを追いながらさらに詳しく説明する。以下の説明において、特に明示しない場合、タグオブジェクトとアクセス制御タグオブジェクトとを総称してオブジェクトと呼ぶ。ユーザは、アクセス要求部１００から、アクセス制御部２００に対してアクセス要求を行う。アクセス要求に伴い引数として、ここではオブジェクト識別名Ａ、主体識別名Ａ、アクセス種別Ａ、アクセス引数Ａが送られたものとする。ここで、オブジェクト識別名Ａとは、対象オブジェクトを特定する情報であり、オブジェクトＩＤやファイル名のような対象を指す名前、あるいはXPathのように木構造の特定の場所を示すポインタである。主体識別名Ａとは、アクセス主体を特定する情報であり、ユーザ名やプロセス名である。アクセス種別Ａとは、要求する処理の首里を特定する情報であり、読込みや書込みのような操作名である。アクセス引数Ａは、操作を規定するために使われるパラメータである。

【００４１】アクセス制御部２００は、アクセス要求を

受け取ると、オブジェクト識別名Ａに対するアクセス情報を取得する為に、オブジェクト識別名Ａを引数として、オブジェクト管理部３００を呼ぶ。

【００４２】オブジェクト管理部３００は、オブジェクト格納部５００の中に、オブジェクト識別名Ａのオブジェクト ＩＤもしくはファイル名に一致するオブジェクトＡが格納されているかどうかを調べる。一致するものがあれば、オブジェクト格納部５００からオブジェクトＡを取得する。ここで、オブジェクトＡは、タグオブジェクト、アクセス制御タグオブジェクト、タグ無しオブジェクトの中の何れかである。オブジェクト格納部５００の中に、オブジェクト識別名Ａに相当するオブジェクトが存在しなかった場合には、エラーを出力して処理を終了する。オブジェクト管理部３００はさらに、オブジェクトＡにアクセス制御識別名タグが存在していた場合、そのタグに書かれたデータをオブジェクト識別名Ｂとみなし、再度オブジェクト格納部５００からオブジェクト識別名Ｂに該当するオブジェクトＢをオブジェクトＡに対するアクセス制御規則として取得する。オブジェクト制御識別タグが複数の場合には、取得すべきオブジェクトＢが複数であるものとする。また、オブジェクトＡにアクセス可能主体というタグ名があれば、当該オブジェクトに対してアクセスできるのが当該アクセス可能主体のみであるため、ここではこれ以上の処理を行わない。オブジェクト管理部３００は、以上のようにして得られたオブジェクトＡ及びオブジェクトＢをアクセス制御部２００に戻す。

【００４３】アクセス制御部２００は、オブジェクトＢに記述されたオブジェクトＡに対するアクセス制御規則に基づきアクセス判定を行う。そして、得られたアクセス判定結果に基づき、アクセス処理部６００に対して必要な処理を依頼する。

【００４４】アクセス処理部６００は、図４に示したように、アクセス制御部２００から対象オブジェクトと、アクセス対象タグ、アクセス種別タグ、及びアクセス判定結果を示すアクセスフラグタグを受け取り、これらに基づいて対象オブジェクトに対する処理を実行する。そして、処理の結果に応じて結果オブジェクトＲを生成し、アクセス制御部２００に送る。

【００４５】アクセス制御部２００は、アクセス処理部６００において生成された結果オブジェクトＲを、アクセス要求部１００またはアクセス格納部５００に送る。例えば、アクセス要求にて要求された処理（アクセス種別タグ）が対象オブジェクトのリードであれば、結果オブジェクトＲ（対象オブジェクトと同一）をアクセス要求部１００に返送する。また、アクセス処理部６００においてデータの書き換えが行われたならば、生成された結果オブジェクトＲをアクセス処理部６００へ送って格納する。また、処理の内容によっては、アクセス要求部１００及びアクセス格納部５００の両方に結果オブジェクトＲを送る場合もあるし、何もしない場合もある。これらの判断は、例えば、アクセス制御部２００において、図８に示すような対応テーブルを持っておき、アクセス要求の引数であるアクセス種別またはアクセス制御タグオブジェクトのアクセス種別タグに応じて決定することができる。

【００４６】次に、オブジェクト格納部５００から取得されたオブジェクトＡがタグ無しオブジェクトであった場合について説明する。この場合、タグ無しオブジェクトはタグを持たないため、アクセス制御規則を記述したアクセス制御タグオブジェクトを指示することができない。そこで、オブジェクト対応管理部４００により補足処理を行う。この場合、オブジェクト管理部３００は、オブジェクト対応管理部４００に対してオブジェクト識別名Ａに対応するアクセス制御を指定したエントリーがあるかどうかを問い合わせる。オブジェクト対応管理部４００は、オブジェクト管理部３００から問い合わせられたエントリーに対応するアクセス制御タグオブジェクトがあれば、オブジェクト管理部３００に対してそのオブジェクトの識別名を戻す。ここでは、オブジェクト識別名Ｂが戻されたものとする。また、オブジェクト管理部３００から問い合わせられたエントリーに対応するアクセス制御タグオブジェクトがない場合には、何も記述がされていない空のアクセス制御タグオブジェクトを戻す。また、オブジェクト対応管理部４００は、管理するエントリーの有効期限や使用フラグに基づいてエントリーの削除等の管理をも行う。オブジェクト対応管理部４００に格納されているタグ無しオブジェクトとアクセス制御タグオブジェクトとの対応関係の詳細については後述する。

【００４７】次に、アクセス制御部２００におけるアクセス制御の判定を行う処理について詳細に説明する。オブジェクト管理部３００から送られてきたアクセス制御タグオブジェクトには、アクセス対象、アクセス主体、アクセス種別、アクセスフラグ、アクセス許可条件が記述されている。図５は、アクセス要求部１００から送られたアクセス要求に対するアクセス判定アルゴリズムを示す図である。図５において、まず、アクセス要求に応じて取得された主体識別名Ａ、アクセス種別Ａ、アクセス主体、アクセス種別、アクセスフラグ、アクセス許可条件の各データがオブジェクト管理部３００から送られてくる（ステップ８０１）。次に、主体識別名Ａがアクセス主体に含まれている規則を全て抽出する（ステップ８０２）。ここで、規則がない場合はアクセス不許可となる（ステップ８０８）。主体識別名Ａがアクセス主体に含まれているものがあれば、次の処理として、その中でさらにアクセス種別Ａがアクセス種別に含まれている規則を全て抽出する（ステップ８０３）。ここで、規則がない場合はアクセス不許可となる（ステップ８０８）。アクセス種別Ａがアクセス種別に含まれているものがあれば、

次の処理として、その中でアクセス条件が満足されるものを全て抽出する(ステップ８０４)。ここで、規則がない場合はアクセス不許可となる(ステップ８０８)。アクセス条件が満足されるものがあれば、次の処理として、抽出された規則の中で最も優先度の高い規則を選択する(ステップ８０５)。次に、選択された規則は一つあるいは複数だが、アクセスフラグは全て同一であるかどうかの判断を行う(ステップ８０６)。アクセスフラグが全て同一でない場合には、アクセス不許可となる(ステップ８０８)。アクセスフラグが全て同一であれば、次の処理として、それらの規則においてアクセスフラグが許可であるかどうかの判定を行う(ステップ８０７)。アクセスフラグが不許可であればアクセス不許可となる(ステップ８０８)。ステップ８０７にて、アクセスフラグが許可である場合にはアクセス許可となる(ステップ８０９)。

【００４８】次に、タグ無しオブジェクトをアクセス制御するためのオブジェクト管理部３００と、オブジェクト対応管理部４００における処理について説明する。オブジェクト管理部３００に送られてきたタグオブジェクトの中に、タグ無しオブジェクトの識別子が含まれている場合に、オブジェクト管理部３００は、オブジェクト対応管理部４００に対して新しくエントリーを生成するように要求する。これは、ＨＴＭＬファイル等のタグオブジェクトに対するアクセスが行われ、その直後に当該gifファイルやWordファイル等のタグ無しオブジェクトに対するアクセスが発生した場合に対処するために行う。本実施の形態では、タグ無しオブジェクトに対するアクセス制御規則は当該タグ無しオブジェクトがポイントされているタグオブジェクト経由でアクセス制御を行うことを前提とする。従って、タグオブジェクトに含まれるタグ無しオブジェクトと対応するアクセス制御規則をオブジェクト対応管理部４００に送り、一時的に対応表を作成するようにする。この表により、ＨＴＭＬファイル等のタグオブジェクトが読まれた直後の、gifファイル等のタグ無しオブジェクトの読込みアクセスを柔軟な制御を行うことができる。

【００４９】オブジェクト対応管理部４００におけるオブジェクト対応管理処理について説明する。オブジェクト対応管理部４００は、タグ無しオブジェクトとアクセス制御規則の関係を一時的に保管するためのオブジェクト対応テーブルを管理する。図６はオブジェクト対応テーブルの構成例を示す図である。図６を参照すると、オブジェクト対応テーブルには、オブジェクト識別子、アクセス主体、アクセス種別、アクセス制御タグオブジェクト識別子、有効期限、履歴といったデータ項目とインターフェイスの定義とを関係付けて構成される。オブジェクト識別子は、タグ無しオブジェクトの識別子であり、例としてはgifファイル(.gif)等が挙げられる。アクセス制御タグオブジェクト識別子は、オブジェクト識別子に対するアクセス制御規則であり、どの規則を使ったかが判るものである。これらのデータ項目の他に、各エントリーの有効期限や使用履歴の示すフラグなどを設定し、各エントリーの有効期限や使用履歴等の情報から、有効期限の過ぎたエントリーの削除等を行い、オブジェクト対応テーブルの管理を行う。

【００５０】アクセス処理部６００は、アクセス種別によって定められた必要処理をオブジェクトに対して実行する。ここで、必要処理とは、アクセス処理部６００に格納されているスクリプトプログラム、及びデフォルトで提供されているプログラムによって構成されているものとする。また、このスクリプトプログラムは、引数としてオブジェクト、アクセス種別、アクセス引数を使う。スクリプトプログラムは、要求に応じた処理結果を処理済みオブジェクトとして戻す機能を持つ。図７にアクセス処理部６００における必要処理の例を示す。デフォルトで提供されているプログラムは、新しくオブジェクトを生成する際にアクセス可能主体タグとアクセス制御識別タグの値をセットするプログラムと、オブジェクトを削除する際に中身のないヌルオブジェクトを作るプログラムである。前者は、アクセス可能主体タグにアクセス要求のアクセス主体識別名を、アクセス制御識別タグにアクセス制御タグオブジェクト識別子をセットするプログラムである。

【００５１】またここで、オブジェクト管理部３００からアクセス制御部２００に対してタグオブジェクトが送られた際、送られてきたアクセス制御タグオブジェクトの中には、複数のアクセス制御規則が記述されている場合が考えられる。あるいは、オブジェクト管理部３００からは、複数のアクセス制御タグオブジェクトが送られてくる可能性がある。その場合、アクセス制御規則同士で矛盾が発生する可能性がある。例えば、第一の規則で、『AliceはDateタグの内容をReadできる』と書かれているのに、第二の規則で、『AliceはDateタグの内容をReadできない』と書かれているような場合である。そこで、本アルゴリズムは、規則間の優先順位に基づいた矛盾解決方法を用いる。各規則に優先順位を設定し、常に優先順位の高いアクセス制御規則が適用されることとする。この場合、規則群の全ての規則に対して各々異なる優先度を割り当てれば、必ず矛盾しない結果が得られることは明らかである。

【００５２】図９に社員データに対するアクセス制御規則の例を示す。ここで、ＩＤ＝１の規則は、『人事課長は社員の給料フィールドを変更できる』ことを示し、ＩＤ＝２の規則は、『社員の役職がない場合、人事課長は社員の給料フィールドを変更できない』ことを示している。このような場合、ＩＤ＝１の規則から『変更可能』、ＩＤ＝２の規則から『変更不能』といったように、ＩＤ＝１とＩＤ＝２の規則は変更権限に関して矛盾した結果を出力する可能性がある。本実施の形態では、

各規則に付けた優先度に基づいて、矛盾解消を行う。図９に示すように、規則１には優先度２（ＰＲ＝２）、規則２には優先度１（ＰＲ＝１）を属性として設定した。つまり、『変更不能』と設定した規則の優先度の方が、『変更可能』と設定した規則の優先度よりも高いので、『変更不能』という結果が得られることになる。このように、権限に矛盾が発生した場合でも、優先度から規則を判定することができる。

【００５３】次に、既に存在するタグオブジェクトに対する変更動作をどのようにアクセス制御するかを具体的な例を用いて更に詳しく説明する。オブジェクト内のデータに対する変更動作は変更、あるいは追加というアクセス種別で表現する。ここで変更とは、タグオブジェクト内のタグ構造を変更することを意味する。追加とは、タグオブジェクト内に新しく子供のタグ構造を追加することを意味する。

【００５４】図１０は、データ及びアクセス制御規則の初期状態を表している。図１０において、各タグオブジェクトに付されたオブジェクト１、オブジェクト２、オブジェクト３は、オブジェクト識別名である。オブジェクト識別名がオブジェクト１であるオブジェクトは、Aliceという社員の給料に関する内容の情報を持つタグオブジェクトである。また、オブジェクト識別名がオブジェクト２であるオブジェクトは、タグオブジェクトに対するアクセス制御規則群を表すアクセス制御タグオブジェクトである。さらに、オブジェクト識別名がオブジェクト３であるオブジェクトは、アクセス制御タグオブジェクトに対するアクセス制御規則を表すアクセス制御タグオブジェクトである。オブジェクト３には、アクセス可能主体に相当する変更可能者が指定されている、また、同図において、太い矢印はアクセス制御識別名タグの値を示しており、自オブジェクトに対するアクセス制御規則を記述するオブジェクトを指している。細い矢印はアクセス制御を行うことのできる対象範囲を示している。

【００５５】次に、タグオブジェクトに対してアクセス制御を行う場合の動作を説明する。図１１は、図１０に示した関係のオブジェクト群において、タグオブジェクトにデータを追加する様子を説明する図である。図１１の例では、アクセス要求部１００から、オブジェクト識別名Ａが『オブジェクト１』、主体識別名Ａが『人事課長』、アクセス種別Ａが『追加』、アクセス引数Ａが『<社員><名前>Bob</名前><給料>２０万</給料></社員>』というアクセス要求があったものとする。アクセス制御部２００は、受け取ったアクセス要求の中からオブジェクト識別名Ａであるオブジェクト１を取り出し、オブジェクト管理部３００に送る。

【００５６】オブジェクト管理部３００は、オブジェクト格納部５００からオブジェクト識別名Ａに相当するオブジェクト１を取り出す。取り出されたオブジェクト１であるタグオブジェクトから、当該タグオブジェクトのアクセス制御識別名タグで示されるアクセス制御タグオブジェクトの識別名を取り出す。ここで取り出される識別名にて特定されるアクセス制御タグオブジェクトは、当該オブジェクト１であるタグオブジェクトに対するアクセス制御規則を規定する。ここでは、太い矢印で示されるオブジェクト２である。オブジェクト管理部３００は、オブジェクト格納部５００からオブジェクト２を取り出す。アクセス制御部２００は、データを表すオブジェクト１とアクセス制御規則を表すオブジェクト２とを受け取り、アクセス要求部１００からのアクセス引数Ａとともに、アクセス処理部６００へ送る。

【００５７】アクセス処理部６００は、オブジェクト２が人事課長によってオブジェクト１に対するアクセス引数Ａを追加することを許可しているかどうかを検証する。そして、規則１が社員データに対して人事課長がデータを追加することができることが書かれている規則であることを確認し、追加処理を行う。これにより、アクセス要求部１００からアクセス引数Ａとしてアクセス要求があった、社員データであるオブジェクト１対するBobの社員エントリーの追加がなされる。更新されたオブジェクト１は、オブジェクトＲとしてアクセス制御部２００に送られる。

【００５８】アクセス制御部２００は、アクセス種別に応じて、更新されたオブジェクト１であるオブジェクトＲをアクセス要求部１００に送り返すか、オブジェクト管理部３００に送るかを決定する。オブジェクトＲの送り先は、例えば上述した図８に示すような対応テーブルにより、アクセス処理部６００にて行われた処理の内容に基づいて決定される。ここでは、アクセス種別が追加の場合に、作成されたオブジェクトＲをオブジェクト管理部３００に送るという規則があるものとし、社員エントリーの追加がなされたオブジェクト１であるオブジェクトＲをオブジェクト管理部３００に送る。オブジェクト管理部３００は、アクセス制御部２００から受け取ったオブジェクトＲをオブジェクト格納部５００に送り、格納する。最後に、アクセス制御部２００は、アクセス判定結果をアクセス要求部１００に送り、アクセス要求に対する処理を終了する。

【００５９】次に、アクセス制御規則に対してアクセス制御を行う場合の動作を説明する。図１２は、図１１の状態にあるオブジェクト群において、アクセス制御タグオブジェクトにアクセス制御規則を追加する様子を説明する図である。図１２の例では、アクセス要求部１００から、オブジェクト識別名Ａが『オブジェクト２』、主体識別名Ａが『人事部長』、アクセス種別Ａが『追加』、アクセス引数Ａが『<規則>[名前、監査課、読み]</規則>』というアクセス要求があったものとする。ここで、『[名前、監査課、読み]』の各部分はそれぞれ、『名前』がアクセス対象タグ、『監査課』がアクセス主

体タグ、『読み』がアクセス種別タグを表現しているものとする。アクセスフラグタグには許可、アクセス条件タグには真が指定されていると仮定する。アクセス制御部２００は、受け取ったアクセス要求の中からオブジェクト識別名Ａであるオブジェクト２を取り出し、オブジェクト管理部３００に送る。

【００６０】オブジェクト管理部３００は、オブジェクト格納部５００からオブジェクト識別名Ａに相当するオブジェクト２を取り出す。取り出されたオブジェクト２であるアクセス制御タグオブジェクトから、アクセス制御識別タグで示されるアクセス制御タグオブジェクトの識別名を取り出す。個々で取り出される識別名にて特定されるアクセス制御タグオブジェクトは、当該オブジェクト２であるアクセス制御タグオブジェクトに対するアクセス制御規則を規定する。ここでは、太い矢印で示されるオブジェクト３である。オブジェクト管理部３００は、オブジェクト格納部５００からオブジェクト３を取り出す。アクセス制御部２００は、アクセス制御規則を表すオブジェクト２とアクセス制御規則に対するアクセス制御規則を表すオブジェクト３とを受け取り、アクセス要求部１００からのアクセス引数Ａとともに、アクセス処理部６００へ送る。

【００６１】アクセス処理部６００は、オブジェクト３が人事部長によってオブジェクト２に対するアクセス引数Ａを追加することを許可しているかどうかを検証する。そして、管理１がオブジェクト２のアクセス制御規則の規則群に対して新たなアクセス制御規則を追加することができるということが書かれている規則であるということを確認し、追加処理を行う。これにより、アクセス要求部１００からアクセス引数Ａとしてアクセス要求があった、オブジェクト２に対する規則３のエントリーの追加がなされる。更新されたオブジェクト２は、オブジェクトＲとしてアクセス制御部２００に送られる。

【００６２】アクセス制御部２００は、アクセス種別に応じて、更新されたオブジェクト２であるオブジェクトＲをアクセス要求部１００に送り返すか、オブジェクト管理部３００に送るかを決定する。上述したように、アクセス種別が追加の場合には、作成されたオブジェクトＲをオブジェクト管理部３００に送るという規則があるものとし、規則３のエントリーの追加がなされたオブジェクト２であるオブジェクトＲをオブジェクト管理部３００に送る。オブジェクト管理部３００は、アクセス制御部２００から受け取ったオブジェクトＲをオブジェクト格納部５００に送り、格納する。最後に、アクセス制御部２００は、アクセス判定結果をアクセス要求部１００に送り、アクセス要求に対する処理を終了する。

【００６３】以上のプロセスで示したように、データに対するアクセス制御と、アクセス制御規則に対するアクセス制御規則を同一に扱うことができる。なお、全てのタグオブジェクトの上位に存在するアクセス制御タグオブジェクトには、必ずアクセス可能主体が書かれているものとする。すなわち、本実施の形態によるアクセス制御システムにおいても、全てのオブジェクトに対する権限を持つユーザが設定されることになる。ただし、上記のようにアクセス制御規則を多重化し、柔軟に設定できるため、特定のアクセス制御規則に対するアクセス権限の一部のみを特定のユーザに与えようとする場合にも、そのようなアクセス制御規則をアクセス制御タグオブジェクトの形式で設定すれば良く、当該権限を与えようとするユーザをアクセス可能主体に加える必要はない。図１０乃至図１２に示した例では、最上位のアクセス制御タグオブジェクトとしては、オブジェクト３が該当し、アクセス可能主体（図では変更可能者と記載）としては、人事システム担当者が記述されている。

【００６４】次に、タグオブジェクトの生成、削除の制御について、具体的な例を用いて説明する。タグオブジェクトの生成処理は生成というアクセス種別で表現し、削除処理は削除というアクセス種別で表現する。図１３に初期状態を示す。図１３においてオブジェクト１、オブジェクト２はオブジェクト識別名を表す。オブジェクト１は社員情報を表現するタグオブジェクトであり、オブジェクト２はオブジェクト１へのアクセスを制御するアクセス制御タグオブジェクトである。オブジェクト２には、アクセス主体が『正社員』グループならば社員情報タグの下位に新しくタグを生成できるという規則と、オブジェクト２の生成者は、社員情報タグの中に書かれた要素内容を削除できるという規則を表す。ここでいう、削除とはタグの削除、またはタグも含めたオブジェクトの構成要素全体の削除のどちらかを意味することになる。

【００６５】まず、タグオブジェクトの生成を要求するアクセス制御要求について詳しく説明する。図１４は、図１３の状態から新規のタグオブジェクト（オブジェクト識別名がオブジェクト３）を生成する様子を説明する図である。アクセス要求部１００から、オブジェクト識別名Ａが『オブジェクト１』、主体識別名が正社員フループに含まれる『鈴木』、アクセス種別Ａが『生成』、アクセス引数Ａが『<情報><PDA>WorkPad</PDA></情報>』というアクセス要求があったものとする。これに応じて、アクセス制御部２００は、アクセス要求からオブジェクト識別名Ａである『オブジェクト１』を取り出し、オブジェクト管理部３００に送る。

【００６６】オブジェクト管理部３００は、オブジェクト格納部５００からオブジェクト１を取り出す。オブジェクト管理部３００はオブジェクト１のアクセス制御識別名タグがオブジェクト２をポイントしているので、オブジェクト格納部５００からオブジェクト識別名Ａに相当するオブジェクト２を取り出す。そして、取り出したオブジェクト１及びオブジェクト２をアクセス制御部２００へ送る。

【００６７】アクセス制御部２００は、オブジェクト管理部３００からオブジェクト1及びオブジェクト２を受け取り、図５に示したアクセス判定アルゴリズムを実行し、アクセス許可であることがわかる。したがって、アクセス制御部２００は、アクセス要求部１００からのアクセス引数Ａと共に、オブジェクト1及びオブジェクト２をアクセス処理部６００へ送る。

【００６８】アクセス処理部６００には、図１５に示す処理スクリプトプログラムが設けられているものとする。図１５のタグオブジェクト生成プログラム及びデフォルトのプログラムにより、新しいオブジェクト３が生成され、処理済みオブジェクトとしてアクセス制御部２００に送られる。ここで、オブジェクト3は、自オブジェクトを生成したアクセス制御規則であるオブジェクト２をアクセス制御識別タグの値として持つ。アクセス可能主体の解釈としては、次のようなアクセス制御規則（アクセス制御タグオブジェクト）が存在し、それはアクセス制御識別タグで指定されたオブジェクトより低い優先度を持っていると考えることができる。

〈規則〉

[*、アクセス可能主体名、*]

〈/規則〉

このアクセス制御タグオブジェクトは、該当オブジェクトにアクセス制御識別の値がセットされていない場合は、全ての権限を初期状態で持つものとする。

【００６９】また、図１６に示すように、アクセス種別が生成の場合には、処理済みのオブジェクトの送り先としてオブジェクト格納部５００が設定されているものとする。従って、アクセス制御部２００は、生成されたオブジェクト３をオブジェクト管理部３００に送る。オブジェクト管理部３００は、アクセス制御部２００から受け取ったオブジェクト３をオブジェクト格納部５００に送る。オブジェクト格納部５００は、オブジェクト３をオブジェクト1の社員情報タグの下位に位置するオブジェクトとして蓄える。

【００７０】次に、タグオブジェクトの削除を要求するアクセス制御要求を考える。図１４の状態で、アクセス要求部１００から、オブジェクト識別名Ａが『オブジェクト3』、主体識別名Aが『鈴木』、アクセス種別Aが『削除』というアクセス要求があったものとする。これに応じて、アクセス制御部２００は、アクセス要求からオブジェクト識別名Aである『オブジェクト３』を取り出し、オブジェクト管理部３００に送る。

【００７１】オブジェクト管理部３００は、オブジェクト格納部５００からオブジェクト3を取り出す。オブジェクト管理部３００は、オブジェクト３のアクセス制御識別名タグが、オブジェクト２をポイントしているので、オブジェクト格納部５００からオブジェクト２を取り出す。

【００７２】アクセス制御部２００は、オブジェクト管理部３００からオブジェクト２及びオブジェクト３を受け取り、図５に示したアクセス判定アルゴリズムを実行し、アクセス許可であることがわかる。アクセス制御部２００は、アクセス要求部１００からの各アクセス引数とともに、アクセス処理部６００へ送る。

【００７３】アクセス処理部６００では、空のオブジェクト（Ｎｕｌｌオブジェクト）を生成し、処理済みオブジェクトとする。ここで、図１７に示すように、アクセス種別が削除の場合には、処理済みのオブジェクトの送り先としてオブジェクト格納部５００が設定されているものとする。従って、アクセス処理部２００は、処理済みのタグオブジェクトR（すなわちＮｕｌｌオブジェクト）をオブジェクト格納部５００に送る。オブジェクト格納部５００では、送られてきたＮｕｌｌオブジェクトによって相当するオブジェクト３を上書きし、結果としてオブジェクト３はオブジェクト格納部５００から削除される。このようにして、オブジェクト３が削除された状態を図１８に示す。

【００７４】次に、本実施の形態の適用例として、ＷＥＢサーバ上に保管されたＸＭＬファイルに対してアクセス制御を行う場合の動作例を説明する。図１９は、本実施の形態によるアクセス制御システムを導入したＷＥＢサーバシステムの構成例を示す図である。図１９に示す例では、ＷＥＢサーバ１０００上にオブジェクトとして置かれた複数のＸＭＬファイルに対するアクセス要求を受け付け、当該アクセス要求に対してアクセス制御を行い、その結果をアクセス要求の発信元であるＷＥＢブラウザ２０００にＨＴＭＬ形式のファイルとして提供するサービスを行うものとする。

【００７５】同図において、ＷＥＢブラウザ２０００は、図１におけるアクセス要求部１００に相当する。すなわち、ＸＭＬデータに対するアクセス要求を発行する。特に、本実施の形態では、ＷＥＢブラウザ２０００からのアクセス要求として、アクセス主体を示すユーザ識別名、アクセス対象を示すＸＭＬファイル名、及びアクセス種別名を送る。

【００７６】ＷＥＢサーバ１０００において、送受信部１１００は、ＷＥＢブラウザ２０００から送られたアクセス要求を受け付け、ＸＭＬ－ＨＴＭＬ変換部１２００に送る。また、ＸＭＬ－ＨＴＭＬ変換部１２００から送られたＨＴＭＬファイルをＷＥＢブラウザ２０００に送る。ＸＭＬ－ＨＴＭＬ変換部１２００は、送受信部１１００から送られてきたアクセス要求をアクセス制御部１３００に送る。また、アクセス制御部１３００から送られてきたＸＭＬファイルをＷＥＢブラウザ２０００に返す為に、ＨＴＭＬファイルに変換し、送受信部１１００に送る。アクセス制御部１３００は、図１におけるアクセス制御部２００、オブジェクト管理部３００、オブジェクト対応管理部４００、アクセス処理部６００に相当する。すなわち、アクセス要求として送られてきた各ア

クセス引数に基づいて、アクセスの可否を判定し、アクセス対象であるＸＭＬファイル名を確定し、ＸＭＬデータ格納部１４００から取得する。また、ＸＭＬデータ格納部１４００から取得したＸＭＬファイルをＸＭＬ－ＨＴＭＬ変換部１２００に送る。ＸＭＬデータ格納部１４００は、図１におけるオブジェクト格納部５００に相当する。すなわち、オブジェクトであるＸＭＬファイルを格納する。格納されているＸＭＬファイルには内容が一般のデータであるものと、アクセス制御規則であるものとがある。

【００７７】図２０は、ＸＭＬデータ格納部１４００に格納されているＸＭＬファイルの構成例を示す図である。図２０を参照すると、オブジェクト識別名が、X001.xmlであるタグオブジェクトは、『社員番号１１２２３３のAliceという名前の社員の給料は１０００００円である』という社員オブジェクトについて定義している。Policy.xmlは、社員オブジェクトに対するアクセス制御規則（アクセス制御タグオブジェクト）であり、『人事課員は、社員オブジェクトを読み込みできる』ことを定義している。Admin.xmlは、社員オブジェクトに対するアクセス制御規則であるPolicy.xmlへのアクセス制御規則（アクセス制御タグオブジェクト）であり、『人事課マネージャーは、社員オブジェクトに対するアクセス制御を変更できる』ことを定義している。また、Admin.xmlに記載されたアクセス制御主体は、このアクセス制御タグオブジェクトAdmin.xml自体は、アクセス可能主体である人事システム管理者がアクセス権限を持ち、変更できることを意味する。

【００７８】以上のように、オブジェクト識別名がPolicy.xmlのオブジェクトは、オブジェクト識別名がX001.xmlというデータオブジェクトに対するアクセス制御規則である。また、オブジェクト識別名がAdmin.xmlのオブジェクトは、オブジェクト識別名がPolicy.xmlというアクセス制御規則に対するアクセス制御規則である。これら、Policy.xmlとAdmin.xmlの記述形式には、全く違いがない。このように、本実施の形態によれば、データオブジェクトの定義に対するアクセス制御規則と、アクセス制御規則に対するアクセス制御規則とを区別することなく、オブジェクト間の関係だけから決定できる。

【００７９】これらのアクセス制御タグオブジェクトが用意されている状態で、例えば、ＷＥＢブラウザ２０００から、『人事課員の高橋は社員ファイルを読込みできるか』という質問のアクセス要求があったとする。ここで、アクセス主体は人事課員であるので、この質問に対して、アクセス判定結果としてのアクセスフラグは『許可』である。オブジェクトとしてＸＭＬデータ格納部１４００に格納されている社員ファイルであるX001.xmlがＨＴＭＬファイルに変換されてＷＥＢブラウザ２０００に戻される。

【００８０】また、別の例として、ＷＥＢブラウザ２０００から、『監査課マネージャーの山本は社員ファイルに対するアクセス制御記述を書き換えられるか』という質問のアクセス要求があったとする。ここで、アクセス主体は監査課マネージャーであるので、この質問に対して、アクセス判定結果として『不許可』がＷＥＢブラウザ２０００に戻される。

【００８１】次に、『人事課マネージャーは社員オブジェクトへのアクセス制御規則を変更できる』という規則があったとする。このアクセス制御規則に対して、『監査課マネージャーは社員オブジェクトへのアクセス制御規則の中で、アクセスフラグの部分を変更できる』という規則を追加したとする。これは、監査課マネージャーに対して、社員オブジェクトへのアクセス制御規則の一部の権限を委譲したことを意味する。

【００８２】図２１は、図２０の状態から新たなアクセス制御タグオブジェクトであるＸＭＬファイルを追加した状態を示す図である。図２１において、オブジェクト識別名がPolicy.xmlのオブジェクトは、アクセス制御識別名として、Admin1.xmlとAdmin2.xmlを持つアクセス制御規則であり、『人事課員は社員オブジェクトの読込みができる』ことを意味する。オブジェクト識別名がAdmin1.xmlであるタグオブジェクトは、Policy.xmlに対するアクセス制御規則であり、アクセス可能主体は人事システム管理者である。これは、『監査課マネージャーは、アクセスフラグに対して変更ができる』ことを意味する。オブジェクト識別名がAdmin2.xmlであるタグオブジェクトは、Policy.xmlに対するアクセス制御規則であり、アクセス可能主体は人事システム管理者である。これは、『人事課マネージャーは、アクセス制御に対して変更ができる』ことを意味する。

【００８３】上述したようなアクセス制御規則への変更が発生した後に、ＷＥＢブラウザ２０００から、『監査課マネージャーの山本は社員ファイルに対するアクセス制御記述を書き換えられるか』という質問のアクセス要求があった場合、アクセス判定結果として『許可』がＷＥＢブラウザ２０００に戻され、アクセス制御規則が記述されたファイルであるAdmin1.xmlがＨＴＭＬ形式に変換されてＷＥＢブラウザ２０００に戻される。

【００８４】図２２は、社員オブジェクトX001.xmlと、社員オブジェクトに対するアクセス制御規則であるPolicy.xml、また、アクセス制御規則Policy.xmlに対するアクセス制御規則であるAdmPolicy1.xml及びAdmPolicy2.xmlの各タグオブジェクト間の関係を示す図である。図２２を参照すると、X001.xmlに対するアクセス制御規則がPolicy.xmlであり、Policy.xmlに対するアクセス制御規則がAdmPolicy1.xml及びAdmpolicy2.xmlとなっている。また、データオブジェクトであるX001.xmlに対するアクセス制御規則Policy.xmlの記述形式と、アクセス制御規則であるPolicy.xmlに対するアクセス制御規則AdmPolicy1.xml及びAdmPolicy2.xmlの記述形式との間には、違い

がないことがわかる。

【００８５】このように、従来のアクセス制御においては、『アクセス制御規則を変更できる人は、システム管理者のみ』というような単純な規則があり、この規則は変更できなかった。これに対し、本実施の形態によれば、データオブジェクトに対するアクセス制御規則と同じ記述形式でアクセス制御規則を記述することにより、データオブジェクトに対するアクセス制御規則と、アクセス制御規則に対するアクセス制御規則を区別することなく扱うことができる。アクセス制御規則がデータオブジェクトに対するものか、他のアクセス制御規則に対するものかは、各オブジェクト間の関係だけから決定できる。また、データオブジェクトに対するアクセス制御規則の記述を追加、変更、削除する場合と同様に、アクセス制御規則に対するアクセス制御規則の記述も柔軟に追加、変更、削除することが可能である。

【００８６】次に、本実施の形態における他の適用例として、ＷＥＢサーバ間でＸＭＬファイルをやりとりする場合の動作例を説明する。図２３は、本実施の形態によるアクセス制御システムを導入したＷＥＢサーバと他のＷＥＢサーバとの関係を示す図である。図２３に示す例では、ＷＥＢサーバ３０００上に置かれたＸＭＬで記述された電子注文文書の取得を要求するアクセス要求を他のＷＥＢサーバ４０００から受け付け、当該アクセス要求に対してアクセス制御を行い、その結果をアクセス要求の発信元であるＷＥＢサーバ４０００にＸＭＬ形式のファイルとして提供するサービスを行うものとする。

【００８７】同図において、ＷＥＢサーバ４０００は、図１におけるアクセス要求部１００に相当する。すなわち、ＷＥＢサーバ３０００に対するアクセス要求として、ユーザ識別名、ＸＭＬファイル名、アクセス種別名を送る。

【００８８】ＷＥＢサーバ３０００において、送受信部３１００は、ＷＥＢサーバ４０００から送られたアクセス要求を受け取り、アクセス制御部３２００に送る。また、アクセス制御部３２００から送られたＸＭＬデータをＷＥＢサーバ４０００に送る。

【００８９】アクセス制御部３２００は、図１におけるアクセス制御部２００、オブジェクト管理部３００、オブジェクト対応管理部４００、アクセス処理部６００に相当する。すなわち、送受信部３１００からアクセス要求として送られてきた各アクセス引数に基づいて、アクセスの可否を判定し、アクセス対象であるＸＭＬファイル名を確定し、ＸＭＬデータ格納部３３００から取得する。また、取得したＸＭＬファイルに対するアクセス制御規則をアクセス制御規則格納部３４００から取得する。アクセス制御部３２００にて取得されたＸＭＬデータは、アクセス制御を経た後、送受信部３１００を介してＷＥＢサーバ４０００に送られる。

【００９０】ＸＭＬデータ格納部３３００及びアクセス制御規則格納部３４００は、図１におけるオブジェクト格納部５００に相当する。すなわち、アクセス対象であるオブジェクトを格納する。ＸＭＬデータ格納部３３００は、データオブジェクトのみを格納しており、アクセス制御規則は格納していない。アクセス制御規則格納部３４００は、ＸＭＬデータ格納部３３００に格納されているデータオブジェクトに対するアクセス制御規則や、アクセス制御規則格納部３４００に格納されている他のアクセス制御規則に対するアクセス制御規則を格納している。

【００９１】ここでは、図１９乃至図２２を参照して説明した例とは違い、アクセス対象であるオブジェクトをデータオブジェクトとアクセス制御規則（アクセス制御タグオブジェクト）とに分け、ＸＭＬデータ格納部３３００とアクセス制御規則格納部３４００とにそれぞれ格納している。これにより、物理的に高度なセキュリティを施されたアクセス制御規則格納部３４００にのみアクセス制御規則を格納するなどのような、柔軟なアクセス制御記述管理が可能となる。また、ＸＭＬデータ格納部３３００とアクセス制御規則格納部３４００とを分けたことにより、アクセス制御規則は、タグ付きオブジェクトの形式で記述されていれば良く、特に、ＸＭＬで記述される必要は無くなる。例えばバイナリー形式のタグ付きオブジェクトとして記述すれば、より高速なアクセス制御処理を実現することもできる。

【００９２】

【発明の効果】以上説明したように、本発明によれば、データに対するアクセス制御規則と、アクセス制御規則に対するアクセス制御規則とを区別することなく扱うことができるため、アクセス制御規則に対するアクセス制御についても、データに対するアクセス制御と同様の柔軟な制御を行うことができるアクセス制御システムを提供することができる。これにより、ユーザに対して、アクセス制御規則に対する権限の任意の一部を与えるようなアクセス制御を容易に行うことが可能となる。また、アクセス制御規則の追加、変更、削除等を容易に行うことが可能となる。

【図面の簡単な説明】

【図１】　本実施の形態における、アクセス制御システムの全体構成を説明するブロック図である。

【図２】　本実施の形態における、動作アルゴリズムの全体概要を表す図である。

【図３】　本実施の形態における、アクセス対象となるオブジェクトのデータ構造を示す図である。

【図４】　本実施の形態における、構成要素間のインターフェイスの定義を説明する図である。

【図５】　本実施の形態における、アクセス要求に対するアクセス判定アルゴリズムを示す図である。

【図６】　本実施の形態における、オブジェクト対応テーブルの構成例を示す図である。

【図７】　本実施の形態における、アクセス処理部による処理であるアクセス種別と処理スクリプトプログラムとの関係を示す図である。

【図８】　本実施の形態における、アクセス処理部により処理を施されたオブジェクトの送り先を定めた規則の一例を示す図である。

【図９】　本実施の形態における、タグオブジェクトとアクセス制御タグオブジェクトの例を示す図である。

【図１０】　本実施の形態における、アクセス制御の動作を説明する図であり、データの初期状態の例を示す図である。

【図１１】　図１０に示した関係のオブジェクト群において、タグオブジェクトにデータを追加する様子を説明する図である。

【図１２】　図１１の状態にあるオブジェクト群において、アクセス制御タグオブジェクトにアクセス制御規則を追加する様子を説明する図である。

【図１３】　本実施の形態における、アクセス制御のうちタグオブジェクトの生成及び削除の動作を説明する図であり、データの初期状態の例を示す図である。

【図１４】　図１３の状態から新規のタグオブジェクトを生成した様子を説明する図である。

【図１５】　本実施の形態における、アクセス種別と処理スクリプトプログラム名の関係の一例を示す図である。

【図１６】　本実施の形態における、アクセス処理部により生成されたオブジェクトの送り先を定めた規則の一例を示す図である。

【図１７】　本実施の形態における、アクセス処理部に＊より削除されたオブジェクト（Ｎｕｌｌオブジェクト）の送り先を定めた規則の一例を示す図である。

【図１８】　図１４の状態からタグオブジェクトを削除した様子を説明する図である。

【図１９】　本実施の形態の適用例として、本実施の形態によるアクセス制御システムを導入したＷＥＢサーバシステムの構成例を示す図である。

【図２０】　図１９の適用例における、ＸＭＬデータ格納部に格納されているＸＭＬファイルの構成例を示す図である。

【図２１】　図２０の状態から新たなアクセス制御タグオブジェクトであるＸＭＬファイルを追加した状態を示す図である。

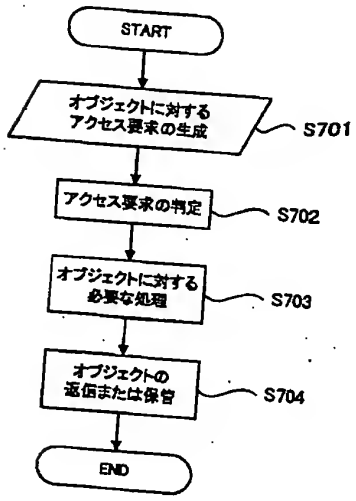
【図２２】　図２０及び図２１に示した各オブジェクトの相互関係を示す図である。

【図２３】　本実施の形態の他の適用例として、本実施の形態によるアクセス制御システムを導入したＷＥＢサーバと他のＷＥＢサーバとの関係を示す図である。

【符号の説明】

１００…アクセス要求部、２００…アクセス制御部、３００…オブジェクト管理部、４００…オブジェクト対応管理部、５００…オブジェクト格納部、６００…アクセス処理部、１０００、３０００、４０００…ＷＥＢサーバ、１１００、３１００…送受信部、１２００…ＸＭＬ－ＨＴＭＬ変換部、１３００、３２００…アクセス制御部、１４００、３３００…ＸＭＬデータ格納部、３４００…アクセス制御規則格納部、２０００…ＷＥＢブラウザ

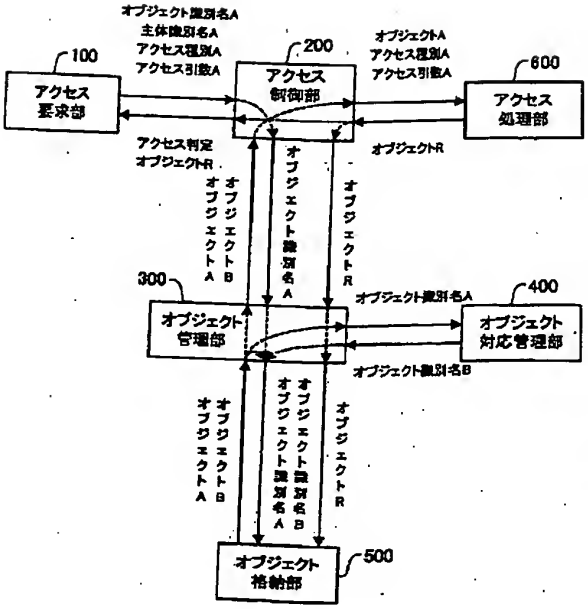
【図2】



【図3】

データの種類	データの構造	意味
タグオブジェクト	アクセス制御識別名タグ	自タグオブジェクトに対するアクセス制御を表現するアクセス制御タグオブジェクトに対する識別名(オブジェクトIDなど)を示す
	アクセス可能主体タグ	自タグオブジェクトを生成したアクセス主体(ユーザ名、システムプロセス番号など)を示す。タグオブジェクトの全てのアクセス種別に対してアクセス権限を持つ。
	任意のタグ	任意のタグを示す。
アクセス制御タグオブジェクト	アクセス制御識別名タグ	同上
	アクセス可能主体タグ	同上
	アクセス対象タグ	アクセス対象のオブジェクトのタグ名
	アクセス主体タグ	アクセスを行うユーザ、グループ、プロセス等の識別子
	アクセス種別タグ	アクセス対象に行う読出し、変更、追加、生成、削除等の処理の種類
	アクセスフラグタグ	"許可"または"不許可"
	アクセス条件タグ	評価可能な式
タグ無しオブジェクト	任意	タグ無しオブジェクトは、任意の形式のオブジェクトであり、内部にタグ表現を持たない。GIFファイルなど。

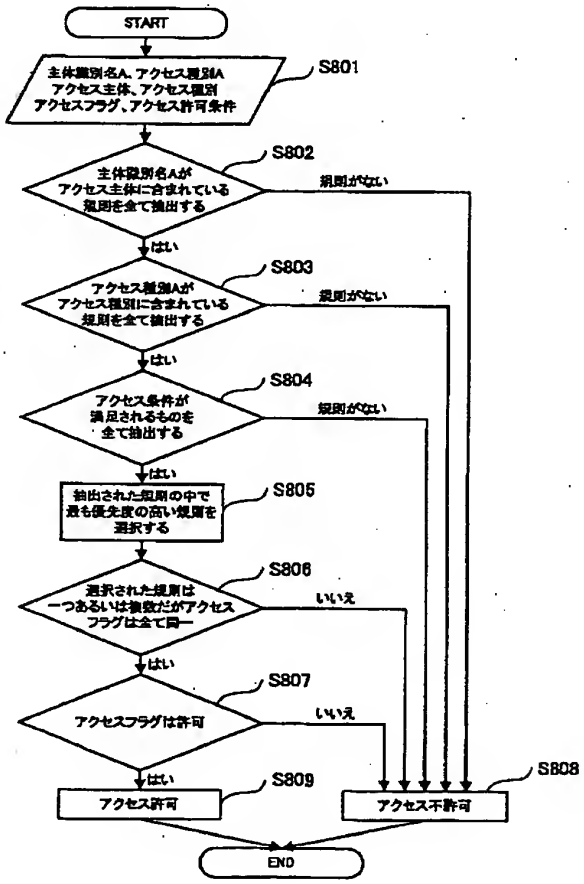
【図１】



【図４】

データの流れる方向	インターフェースの定義
100→200	アクセス要求
200→100	アクセスフラグ(判定結果を表す)、オブジェクト(処理済みオブジェクトを表す)
200→300	オブジェクト識別子(アクセス対象を表す)
200→500	オブジェクト(処理済みオブジェクトを表す)
300→200	アクセスフラグ(対象オブジェクトとアクセス制御タグオブジェクトを表す)
300→500	オブジェクト識別子(アクセス対象を表す)
500→300	オブジェクト(対象オブジェクトまたはアクセス制御タグオブジェクトを表す)
300→400	オブジェクト識別子(アクセス対象、アクセス制御タグオブジェクトを表す)
400→300	オブジェクト(アクセス制御タグオブジェクトを表す)
200→600	オブジェクト、アクセス対象、アクセス種別、アクセスフラグ
600→200	オブジェクト(処理済みオブジェクトを表す)

【図５】



【図６】

データ項目	インターフェースの定義
オブジェクト識別子	タグ無しオブジェクトの識別子
アクセス主体	アクセス主体
アクセス種別	アクセス種別
アクセス制御タグオブジェクト識別子	オブジェクト識別子に対するアクセス制御規則
有効期限	オブジェクト対応表のエントリーの有効期限
履歴	エントリーの履歴を示すフラグ

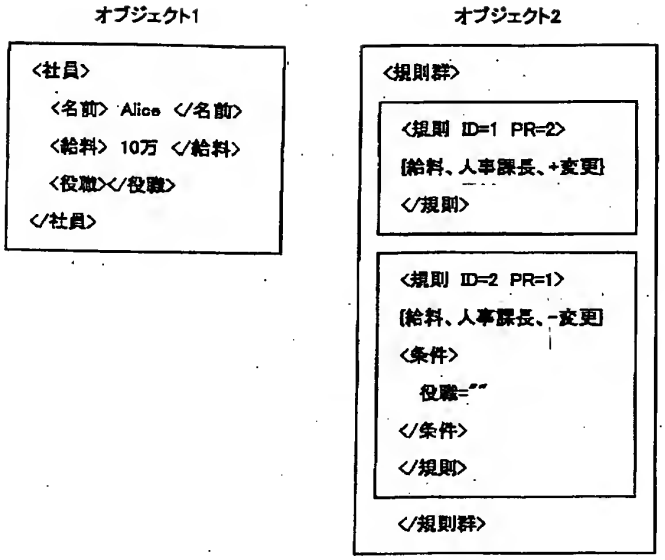
【図７】

アクセス種別	処理スクリプトプログラム名
アクセス種別1	アクセス種別1用プログラム
アクセス種別2	なし
アクセス種別3	アクセス種別3用プログラム

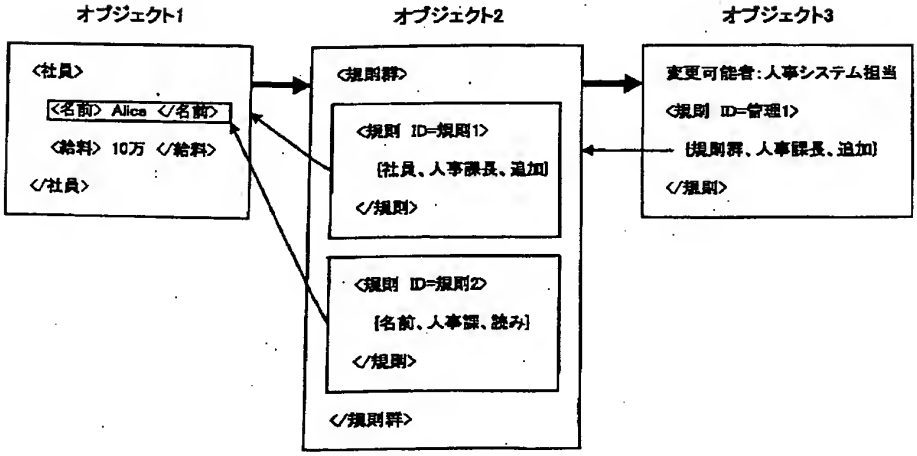
【図８】

アクセス種別	結果オブジェクトの送り先
アクセス種別1	アクセス要求部
アクセス種別2	アクセス制御部
アクセス種別3	オブジェクト管理部、オブジェクト格納部

【図９】



【図１０】



【図１５】

アクセス種別	処理スクリプトプログラム名
生成	タグオブジェクト生成プログラム

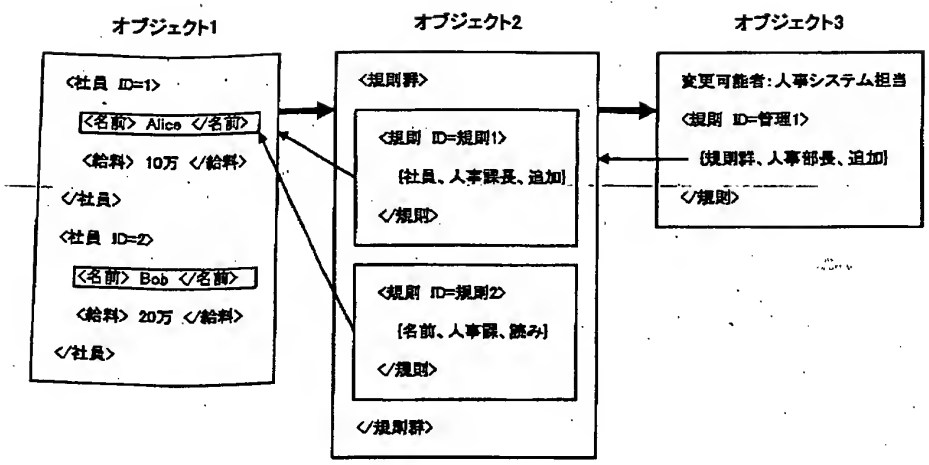
【図１６】

アクセス種別	処理済みオブジェクトの送り先
生成	オブジェクト格納部

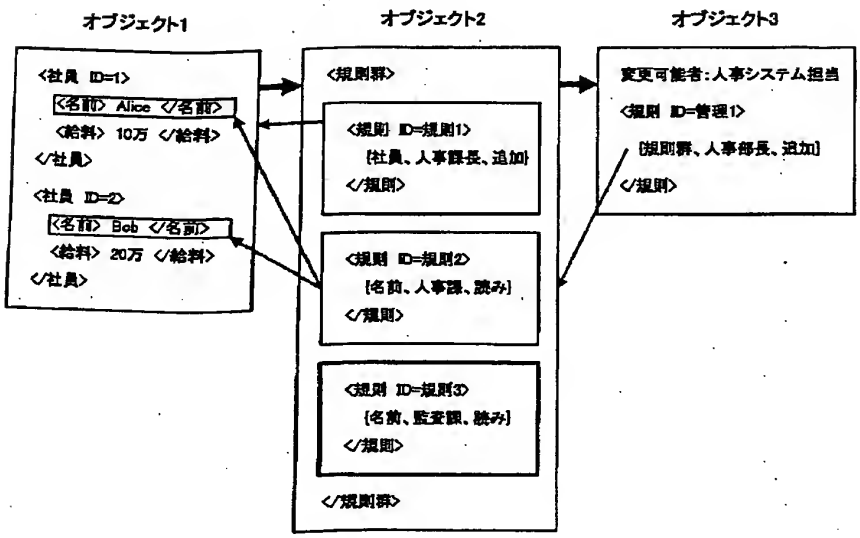
【図１７】

アクセス種別	処理済みオブジェクトの送り先
削除	オブジェクト格納部

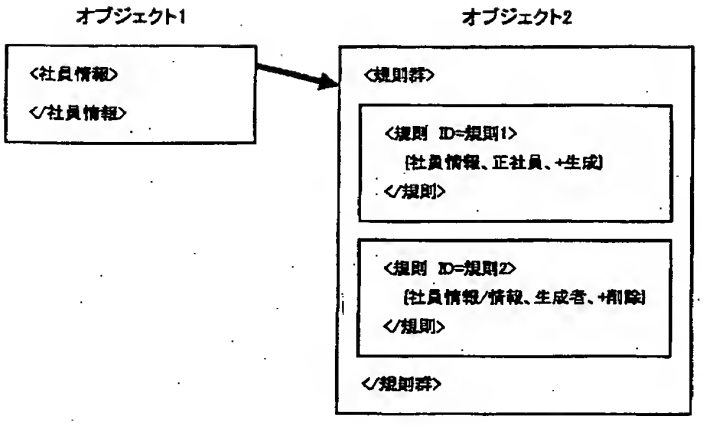
【図１１】


オブジェクト1
<社員 ID=1>
<名前> Alice </名前>
<給料> 10万 </給料>
</社員>
<社員 ID=2>
<名前> Bob </名前>
<給料> 20万 </給料>
</社員>
オブジェクト2
<規則群>
<規則 ID=規則1>
[社員、人事課長、追加]
</規則>
<規則 ID=規則2>
[名前、人事課、読み]
</規則>
</規則群>
オブジェクト3
変更可能者:人事システム担当
<規則 ID=管理1>
[規則群、人事部長、追加]
</規則>

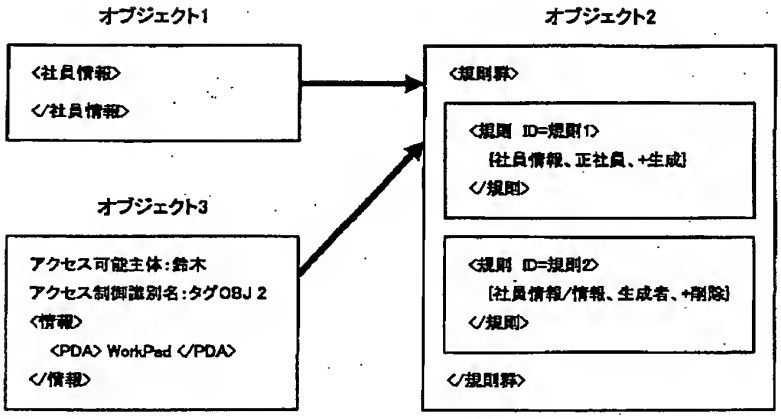
【図１２】


オブジェクト1
<社員 ID=1>
<名前> Alice </名前>
<給料> 10万 </給料>
</社員>
<社員 ID=2>
<名前> Bob </名前>
<給料> 20万 </給料>
</社員>
オブジェクト2
<規則群>
<規則 ID=規則1>
[社員、人事課長、追加]
</規則>
<規則 ID=規則2>
[名前、人事課、読み]
</規則>
<規則 ID=規則3>
[名前、監査課、読み]
</規則>
</規則群>
オブジェクト3
変更可能者:人事システム担当
<規則 ID=管理1>
[規則群、人事部長、追加]
</規則>

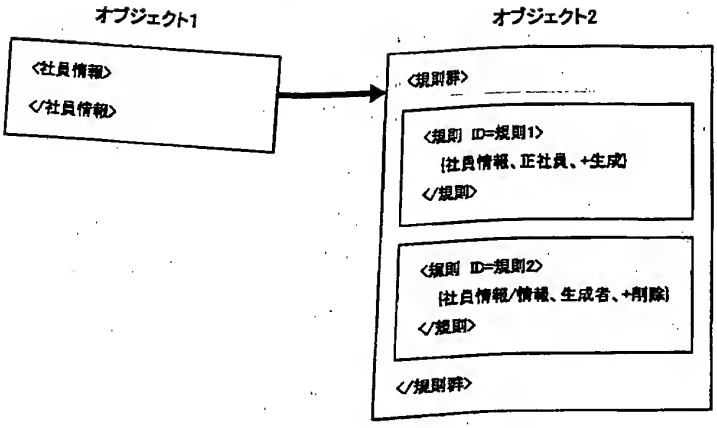
【図１３】


オブジェクト1
<社員情報>
</社員情報>
オブジェクト2
<規則群>
<規則 ID=規則1>
[社員情報、正社員、+生成]
</規則>
<規則 ID=規則2>
[社員情報/情報、生成者、+削除]
</規則>
</規則群>

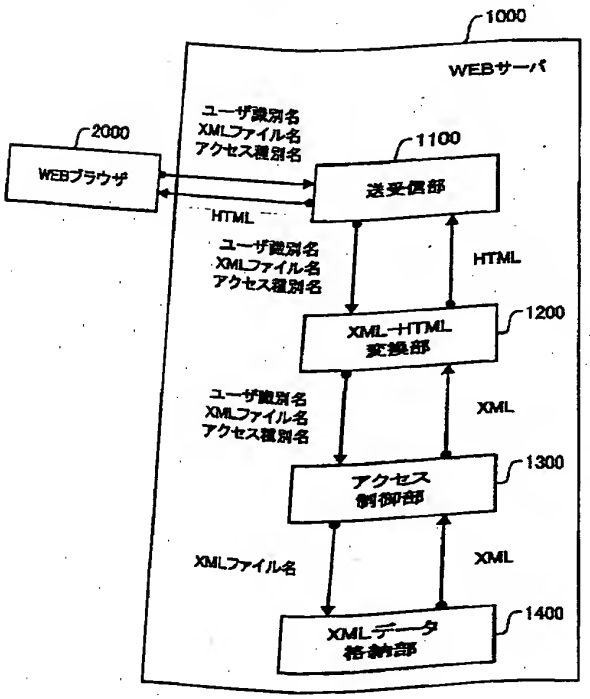
【図１４】


オブジェクト1
<社員情報>
</社員情報>
オブジェクト3
アクセス可能主体:鈴木
アクセス制御識別名:タグOBJ 2
<情報>
<PDA> WorkPad </PDA>
</情報>
オブジェクト2
<規則群>
<規則 ID=規則1>
[社員情報、正社員、+生成]
</規則>
<規則 ID=規則2>
[社員情報/情報、生成者、+削除]
</規則>
</規則群>

【図１８】



【図１９】



【図２０】

オブジェクト識別名：X001.xml

<アクセス制御識別名> Policy.xml </アクセス制御識別名>
<社員>
<名前> Alice </名前>
<社員番号>112233</社員番号>
<給与> 100,000 </給与>
</社員>

オブジェクト識別名：Policy.xml

<アクセス制御先> Admin.xml </アクセス制御先>
<アクセス制御>
<アクセス対象> 社員 </アクセス対象>
<アクセス主体> 人事課員 </アクセス主体>
<アクセス種別> 読込み </アクセス種別>
<アクセスフラグ> 可能 </アクセスフラグ>
<アクセス許可条件></アクセス許可条件>
</アクセス制御>

オブジェクト識別名：Admin.xml

<アクセス可能主体> 人事システム管理者 </アクセス可能主体>
<アクセス制御>
<アクセス対象> アクセス制御 </アクセス対象>
<アクセス主体> 人事課マネージャー </アクセス主体>
<アクセス種別> 変更 </アクセス種別>
<アクセスフラグ> 可能 </アクセスフラグ>
<アクセス許可条件></アクセス許可条件>
</アクセス制御>

【図２１】

オブジェクト識別名：Policy.xml

<アクセス制御識別名> Admin1.xml </アクセス制御識別名>
<アクセス制御識別名> Admin2.xml </アクセス制御識別名>
<アクセス制御>
<アクセス対象> 社員 </アクセス対象>
<アクセス主体> 人事課員 </アクセス主体>
<アクセス種別> 読込み </アクセス種別>
<アクセスフラグ> 可能 </アクセスフラグ>
<アクセス許可条件></アクセス許可条件>
</アクセス制御>

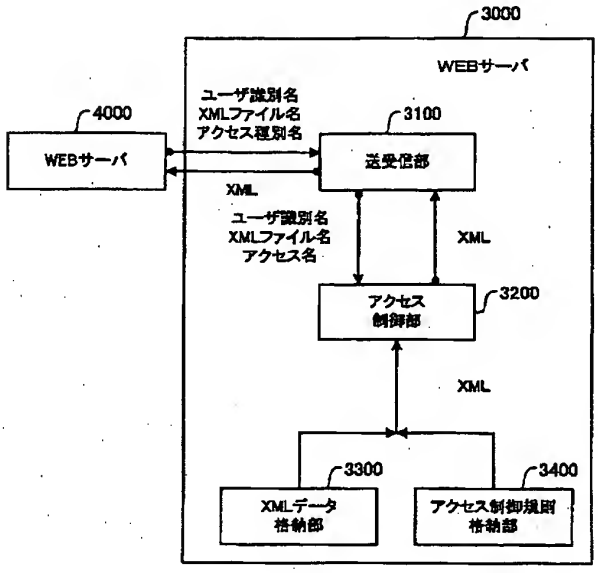
オブジェクト識別名：Admin1.xml

<アクセス可能主体> 人事システム管理者 </アクセス可能主体>
<アクセス制御>
<アクセス対象> アクセスフラグ </アクセス対象>
<アクセス主体> 監査課マネージャー </アクセス主体>
<アクセス種別> 変更 </アクセス種別>
<アクセスフラグ> 許可 </アクセスフラグ>
<アクセス許可条件></アクセス許可条件>
</アクセス制御>

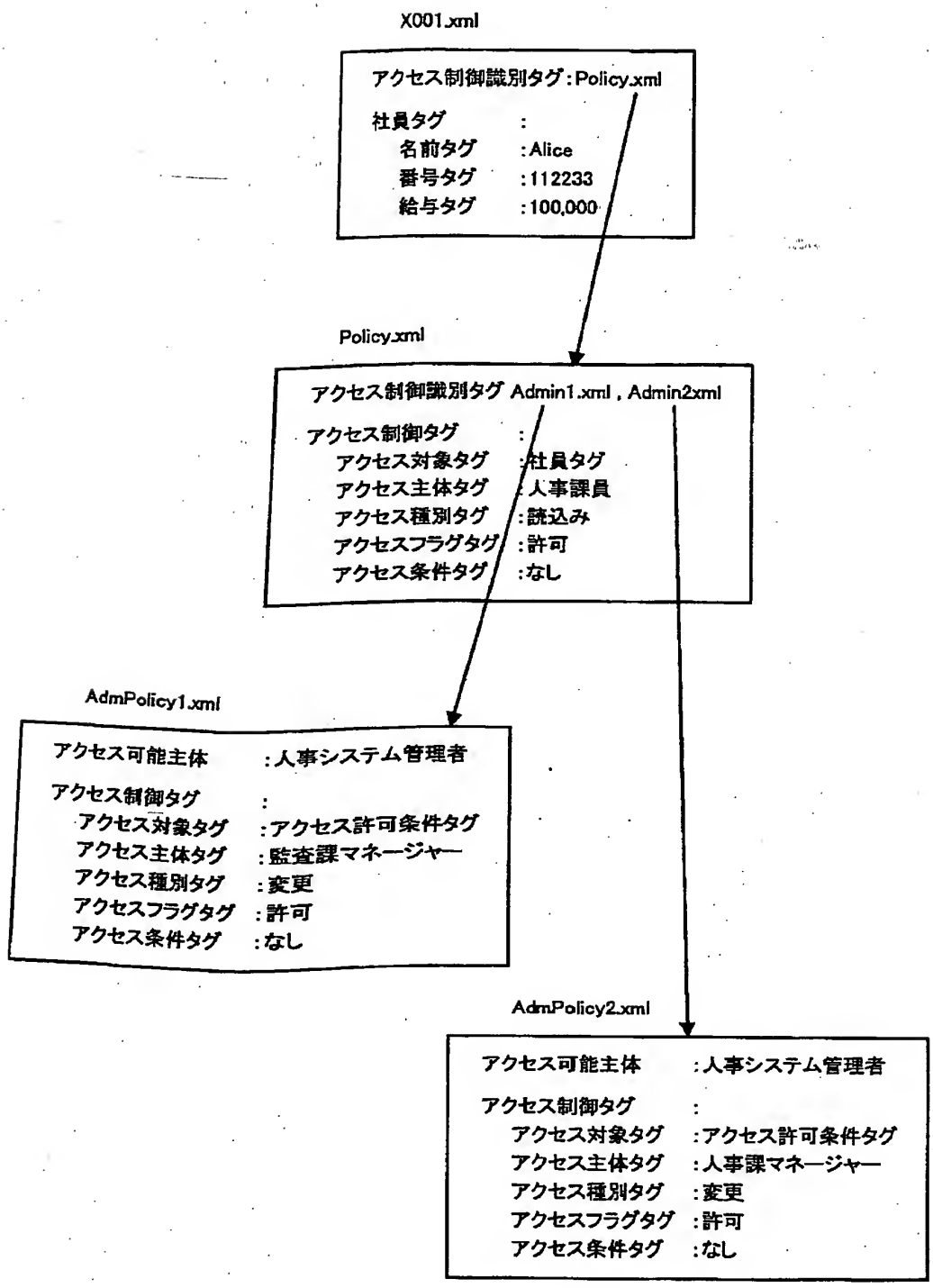
オブジェクト識別名：Admin2.xml

<アクセス可能主体> 人事システム管理者 </アクセス可能主体>
<アクセス制御>
<アクセス対象> アクセス制御 </アクセス対象>
<アクセス主体> 人事課マネージャー </アクセス主体>
<アクセス種別> 変更 </アクセス種別>
<アクセスフラグ> 許可 </アクセスフラグ>
<アクセス許可条件></アクセス許可条件>
</アクセス制御>

【図２３】



【図２２】


X001.xml
アクセス制御識別タグ:Policy.xml
社員タグ :
名前タグ :Alice
番号タグ :112233
給与タグ :100,000
Policy.xml
アクセス制御識別タグ Admin1.xml , Admin2xml
アクセス制御タグ :
アクセス対象タグ :社員タグ
アクセス主体タグ :人事課員
アクセス種別タグ :読込み
アクセスフラグタグ :許可
アクセス条件タグ :なし
AdmPolicy1.xml
アクセス可能主体 :人事システム管理者
アクセス制御タグ :
アクセス対象タグ :アクセス許可条件タグ
アクセス主体タグ :監査課マネージャー
アクセス種別タグ :変更
アクセスフラグタグ :許可
アクセス条件タグ :なし
AdmPolicy2.xml
アクセス可能主体 :人事システム管理者
アクセス制御タグ :
アクセス対象タグ :アクセス許可条件タグ
アクセス主体タグ :人事課マネージャー
アクセス種別タグ :変更
アクセスフラグタグ :許可
アクセス条件タグ :なし

フロントページの続き

(72)発明者 工藤 道治
神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内

(72)発明者 天野 富夫
神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内

Fターム(参考) 5B017 AA01 BA06 BB06 CA16
5B045 BB28 BB48 DD15 GG09 HH02
5B082 GA11